EL 269 994 616 US

6332D-7751

CRYPTOGRAPHIC COMMUNICATION METHOD AND ENCRYPTION METHOD AND CRYPTOGRAPHIC COMMUNICATION SYSTEM

BACKGROUND OF THE INVENTION

Field of the Invention

The present invention relates to a highly secure cryptographic communication method and system, which encrypts and communicates information so that the content of the information is not understood by anyone other than the parties concerned.

Description of the Related Art

In today's so-called advanced information society, important business documents and image data are transmitted/communicated and processed in the form of electronic data over computer networks. Electronic data can be readily reproduced, and it is impossible to distinguish the reproduction from the original, thus placing great importance on the issue of data protection or data security. The realization of computer networks, which satisfy 3 requisites, i.e., "computer resource sharing," "multiple access," and "wide area networking," are essential to the establishment of an advanced information society, but such networks incorporate elements that are inconsistent with the issue of data protection between concerned parties. As an

effective technique for eliminating inconsistencies, attention is focusing on cryptography techniques, which historically have been utilized principally in the military and diplomatic fields.

Cryptography is conversion of information in such a way that the meaning of that information cannot be understood by anyone other than the concerned parties. The conversion of an original text (plaintext), which is capable of being understood by anyone, to a text, the meaning of which is not understood by a third party (ciphertext), is encryption, the changing of ciphertext back into plaintext is decryption, and the overall process of this encryption and decryption is called a cryptographic system. In the encryption process and decryption process, secret data, called, respectively, an encryption key and a decryption key, are utilized. Since a secret decryption key is required for decryption, only a person, who knows this decryption key, can decrypt a ciphertext, enabling the confidentiality of information to be maintained.

An encryption key and decryption key can be alike or different. A cryptographic system, in which both keys are alike, is called a common key cryptographic system, and the DES (Data Encryption Standard) adopted by the National Bureau of Standards (now the National Institute of Standards and Technology) of the United States Department of Commerce is a typical example thereof. As an example of a cryptographic system, in which both keys differ, a cryptographic system called a public key cryptographic system has been proposed. This public key cryptographic system is a cryptographic system, wherein one pair each of an

encryption key and a decryption key are prepared for each user (entity) utilizing the cryptographic system, the encryption key is made public via a public key list, and only the decryption key is kept secret. In a public key cryptographic system, the encryption key and decryption key, which constitute this pair, are different, and the decryption key cannot be deduced from the encryption key by using a one-way function.

A public key cryptographic system is an innovative cryptographic system because it makes the encryption key public. It is also compatible with the above-mentioned 3 requisites needed to establish an advanced information society. In order to utilize the public key cryptographic system in the field of data communications technology, research is being actively carried out, and the RSA cryptographic system has been proposed as a typical public key cryptographic system. This RSA cryptographic system was achieved by a one-way function which makes use of the difficulty of prime factor analysis. Further, various techniques have also been proposed for public key cryptographic systems, which make use of the difficulty associated with solving a discrete logarithm problem (discrete logarithm problem).

Further, a cryptographic system, which makes use of ID (identity) data specific to an individual, i.e. the name, address and the like of each entity, has also been proposed. In this cryptographic system, a common encryption key is generated between sending and receiving parties on the basis of ID data. Further, this ID based cryptographic technique comprises (1) a system, wherein a preliminary communication between the sending and receiving parties is required in advance of ciphertext

communications, and (2) a system, wherein a preliminary communication between the sending and receiving parties is not required in advance of ciphertext communications. It is believed that technique (2) in particular, which does not require a preliminary communication, and is thus very convenient for an entity, will constitute a mainstay of cryptographic systems of the future.

A cryptographic system in accordance with this (2) technique is called ID-NIKS (ID-based non-interactive key sharing scheme), and it adopts a system, wherein the communicating parties share an ID based encryption key and does not perform a preliminary communication. ID-NIKS is a system, wherein sending and receiving parties need not exchange a public-key and secret key, and a key list and third-party service are not required, enabling secure communications to be carried out between the entities.

Fig. 13 of the accompanying drawings illustrates the principle behind this ID-NIKS system. It assumes the existence of a trusted center, and constitutes a shared key generation system having such a center as its core. In Fig. 13, the name, address, telephone number and other ID data of entity X is expressed as h (ID_X) using a hash function h ($\cdot$). The center, based on center public information $\{PC_i\}$, center secret information $\{SC_i\}$, and entity X ID data h (ID_X), computes the following secret information S_{Xi} for an arbitrary entity X, and distributes it secretly to the entity X.

$$S_{Xi} = F_i\ (\{SC_i\},\ \{PC_i\},\ h(ID_X))$$

Entity X, using the secret information of entity X itself $\{S_{Xi}\}$, center public information $\{PC_i\}$, and called-party entity Y ID data h (ID_Y), generates a shared key K_{XY} for encryption and decryption as follows.

$$K_{XY} = f\ (\{S_{Xi}\},\ \{PC_i\},\ h(ID_Y))$$

Further, entity Y also generates a shared key K_{YX} for communication with entity X in the same manner. If there is a relationship $K_{XY} = K_{YX}$ always, these keys K_{XY}, K_{YX} can be used as encryption and decryption keys between entities X and Y.

In the above-described public key cryptographic system, in the case of an RSA cryptographic system, for example, the length of the public key thereof is 11-19 times longer than a current telephone number, and is extremely troublesome to handle. Contrary thereto, in an ID-NIKS, if each ID data is recorded in roster format, shared keys between arbitrary entities can be generated by referencing this roster. Therefore, if an ID-NIKS system like that illustrated in Fig. 13 is securely established, a handy cryptographic system can be constructed on a computer network subscribed to by a number of entities. For this reason, ID-NIKS is expected to form the core of cryptographic systems in the future.

Adequate security against collusion by a plurality of entities and other such attacks is desirable in an ID-NIKS, wherein a shared key, which constitutes an encryption key and a decryption key, is shared in common using the ID data of

the communicating parties without carrying out a preliminary communication. However, an ID-NIKS comprises a problem in that attack methods were studied, and if an adequate number of entities collude, the secret parameters of the center will be disclosed. The ability to construct a cryptographically secure ID-NIKS is an important issue for the advanced information society, and research is being pushed forward on a more ideal cryptographic approach.

Under circumstances such as these, the inventors have proposed an ID-NIKS cryptographic method, which is based on secure and simple ID data, does not require a preliminary communication, and is resistant to collusion attacks (Japanese Patent Application Laid-Open Publication No. 10-210022/1998). This method is characterized in that it has the below-described key-sharing function as a non-separable function, and the basis of the security thereof lies in this characteristic and the difficulty of a discrete logarithm problem.

However, in this ID-NIKS cryptographic method, a special prime number must be utilized (a prime number P, which is specified as P = 2pq + 1 (p, q: large prime numbers)). It has been proven, from a practical standpoint, that this prime number exists in sufficient quantity, but, undeniably, it leaves little freedom in the design of the cryptographic system. Further, the key sharing process must adhere to a 2-stage computing step, and there might be an effective attack method that can be applied during the computing steps, making it vulnerable to attack. These kinds of problems exist with this cryptographic system, leaving room for improvement.

SUMMARY OF THE INVENTION

An object of the present invention is to provide a novel high-security ID-NIKS-based cryptographic communication method and cryptographic communication system, wherein center secret parameters are not disclosed, and ciphertext can not be decrypted even if entities collude with one another.

Another object of the present invention is to provide a cryptographic communication method and a cryptographic communication system, which are capable of solving the problems in the system of prior application Japanese Patent Application Laid-Open Publication No. 10-210022/1998, heightening design freedom, and further enhancing security.

According to a 1st aspect of the present invention, there is provided a cryptographic communication method for communication of information between two entities, wherein an entity-specific secret key is sent to each entity from a center, one entity uses this entity-specific secret key and a public key of the other entity, encrypts a plaintext into a ciphertext, and transmits it to the other entity, and the other entity then decrypts the ciphertext into the original plaintext by using the entity-specific secret key sent from the center and a public key of the above-mentioned one entity, the method being characterized in that cryptographic information is communicated between the two entities using an each entity-specific first key, which is made public as the above-mentioned public key; an each entity-specific secret second key, which is related to the above-mentioned secret key, and which can be determined from the center via a first

function using the first key of each entity; and a third key, which is expressed as a second function having 2 variables (i.e., the one entity's second key and the other entity's first key), and which is shared by both entities, who make use of it when encrypting a plaintext into a ciphertext, and when decrypting a ciphertext into a plaintext, and further characterized in that the first function, which has as parameters an each entity-specific random number controlled or administered by the center, and a third function, which can be obtained by substituting the first function for the second function, and which has the one entity's and the other entity's first keys as variables, are set in the below-defined non-separable function for each respective variable.

Definition: When a suitable commutative operation is treated as O, and function f $(\cdot)$ satisfies f $(x + y) \neq$ f (x) O f (y), function f $(\cdot)$ is characterized as being non-separable in accordance with the operation O.

The second key may comprise a first secret key, which is generated from an each entity-specific first key and a symmetric matrix controlled by the center; a second secret key, which is generated by multiplying a random number by the first secret key; and a third secret key, which is generated on the basis of a random number. Further, the center may send the second and third secret keys to each entity. One entity may then generate a third key using the second and third secret keys and the first key of the other entity.

The following expression may be used as the arithmetic

expression when the center generates the first, second and third secret keys.

$$\vec{x_i} \equiv T^{\vec{v_i}} \pmod{L}$$

$$\vec{s_i} \equiv r_i \cdot \vec{x_i} \pmod{L}$$

$$y_i \equiv g^{r_i^{-e}} \pmod{N}$$

Provided that

Vector v_i: First key of entity i

Vector x_i: First secret key of entity i

Vector s_i: Second secret key of entity i

y_i: Third secret key of entity i

r_i: Random number of entity i

L: $L = \lambda\ (N)$

N: $N = PQ$ (P, Q are prime numbers)

T: Symmetric matrix (Each component is relatively prime to L)

g: Maximum generator over N as a modulus

e: an integer that is relatively prime to L

$\lambda\ (\cdot)$: Carmichael function

The following expression may be used as the arithmetic expression when the one entity generates the third key based on the second and third secret keys and the first key of the other entity.

$$
\begin{aligned}
K_{ij} &\equiv (\cdots((\cdots((\cdots(\overbrace{y_i^{s_{i1}})\cdots)}^{v_{j1}}\overbrace{{}^{s_{i2}})\cdots)}^{v_{j2}}\cdots\overbrace{{}^{s_{in}})\cdots)^{s_{in}}}^{v_{jn}} \\
&\equiv y_i^{\overbrace{s_{i1}\cdots s_{i1}}^{v_{j1}}\overbrace{s_{i2}\cdots s_{i2}}^{v_{j2}}\cdots\overbrace{s_{in}\cdots s_{in}}^{v_{jn}}} \\
&\equiv y_i^{{}^t\overrightarrow{s_i}\,\overrightarrow{v_j}} \\
&\equiv y_i^{\left(\prod_{k=1}^{n} r_i^{v_{ik}}\right)\cdot {}^t\overrightarrow{x_i}\,\overrightarrow{v_j}} \\
&\equiv y_i^{r_i^{\left(\sum_{k=1}^{n} v_{ik}\right)}\cdot {}^t\overrightarrow{x_i}\,\overrightarrow{v_j}} \\
&\equiv y_i^{r_i^{e}\cdot {}^t\overrightarrow{x_i}\,\overrightarrow{v_j}} \\
&\equiv g^{r_i^{-e}\cdot r_i^{e}\cdot {}^t\overrightarrow{x_i}\,\overrightarrow{v_j}} \\
&\equiv g^{{}^t\overrightarrow{x_i}\,\overrightarrow{v_j}} \\
&\equiv g^{{}^t\overrightarrow{v_i}\,\mathrm{T}\,\overrightarrow{v_j}} \pmod{N}
\end{aligned}
$$

The each entity-specific first key may be determined by calculating identification information of each entity using a hash function.

According to a 2nd aspect of the present invention, there is provided an encryption method, wherein an each entity-specific secret key is sent to each entity from a center, and an entity uses this entity-specific secret key sent from the center to encrypt a plaintext into a ciphertext, this encryption method being characterized in that a plaintext is encrypted into a ciphertext using an each entity-specific first key, which has been made public; an each entity-specific secret second key, which is determined in the center in accordance with the first key using a first function; and a third key, which is expressed

by a second function having 2 variables (the second key of the encrypting entity itself and the first key of the other entity, who is the recipient of the ciphertext), and further characterized in that a first function, which has as parameters an each entity-specific random number controlled by the center, and a third function, which can be obtained by substituting the first function for the second function, and which has the one entity's and the other entity's first keys as variables, are set in the below-defined non-separable function for each respective variable.

Definition: When a suitable commutative operation is treated as O, and function $f(\cdot)$ satisfies $f(x + y) \neq f(x) \mathrm{O} f(y)$, function $f(\cdot)$ is characterized as being non-separable in accordance with the operation O.

According to a 3rd aspect of the present invention, there is provided a cryptographic communication system, which comprises a plurality of entities, which reciprocally perform processing for encrypting a plaintext (or information) into a ciphertext and transmitting it to another entity, and processing for decrypting a transmitted ciphertext into an original plaintext; and a center, which sends an each entity-specific secret key to each entity, this cryptographic communication system being characterized in that the center determines each entity-specific secret second keys in accordance with a first function from an each entity-specific first key that has been made public, and the plurality of entities determine a third key, which is expressed by a second function having 2 variables of the one entity's second key and the other entity's first key, and which is used

when encrypting a plaintext into a ciphertext, and when decrypting a ciphertext into a plaintext, and further characterized in that a first function, which has as parameters an each entity-specific random number controlled by the center, and a third function, which can be obtained by substituting the first function for the second function, and which has the one entity's and the other entity's first keys as variables, are set in the below-defined non-separable function for each respective variable.

Definition: When a suitable commutative operation is treated as $\circ$, and function $f(\cdot)$ satisfies $f(x + y) \neq f(x) \circ f(y)$, function $f(\cdot)$ is characterized as being non-separable in accordance with the operation $\circ$.

The second key may comprise a first secret key, a second secret key, and a third secret key. Further, the center may include means for calculating the first secret key from each entity-specific first key and a symmetric matrix controlled by the center; means for calculating the second secret key by multiplying the first secret key by a random number; and means for calculating the third secret key on the basis of the above-mentioned random number, and may send the calculated second and third secret keys to each entity.

Each of the entities may include means for calculating the third key from the second and third secret keys sent from the center, and the first key of the other entity (i.e., communicating party).

The concept of the ID-NIKS of the cryptographic communication method of the present invention is described hereinbelow.

First, separability in a function is defined as follows by generalizing the concept of linearity. When a suitable commutative operation is treated as O, and function f (·) satisfies the following relational expression, this function f (·) is defined as being separable in accordance with the operation O.

$$f\ (x + y) = f\ (x)\ \mathrm{O}\ f\ (y)$$

For example, $f\ (x) = ax$ and $f\ (x) = a^x$ are separable as shown below.

$$f\ (x + y) = a\ (x + y) = ax + ay = f\ (x) + f\ (y)$$

$$f\ (x + y) = a^{x + y} = a^x \cdot a^y = f\ (x) \cdot f\ (y)$$

The definition of the power computation of a matrix is as shown below. Provided that each matrix A, B, C is treated as a matrix of m x 1, 1 x n, m x n, respectively.

Define the matrix right power computation $C = A^B$ as

$$c_{ij} = \prod_{k=1}^{\ell} a_{ik}{}^{b_{kj}} \quad (i = 1, 2, \ldots, m, \quad j = 1, 2, \ldots, n)$$

Define the matrix left power computation $C = {}^{A}B$ as

$$c_{ij} = \prod_{k=1}^{\ell} b_{kj}{}^{a_{ik}} \quad (i = 1, 2, \ldots, m, \quad j = 1, 2, \ldots, n)$$

Further, an operation *, which finds the product for each component of a matrix, is defined as shown below. Provided that each matrix A, B, C is treated as an m x n matrix.

Define the component products of matrix $C = A * B$ as

$c_{ij} = a_{ij}b_{ij}$ ($i = 1, 2, \ldots, m$, $j = 1, 2, \ldots, n$).

In accordance with the above definitions, the following properties are achieved. Provided that t signifies the matrix transposition.

$$1.\ {}^t\left(A^B\right) = {}^{tB}\,{}^tA$$

$$2.\ \left(A^B\right)^C = A^{BC}$$

$$3.\ \left({}^A B\right)^C = {}^A\left(B^C\right)$$

$$4.\ (A * B)^C = A^C * B^C$$

$$5.\ A^{(B+C)} = A^B * A^C$$

Next, conditions for achieving ID-NIKS, and conditions for a secure ID-NIKS are considered. Provided that i, j, y and z represent entities, v_i is treated as the public key of entity i ("first key" in the claims), which is an ID hash value in most cases, s_i is treated as a secret key of entity i ("second key"), and K_{ij} is treated as an entity i-determined key shared with entity j ("third key").

The following 3 conditions are required for achieving ID-NIKS.

<u>Condition 1 (Secret Key Condition):</u>

A center can determine a secret key s_i from a corresponding public key v_i of entity i using a secret-key function $f(\cdot)$ ("first function").

$s_i = f(v_i)$

<u>Condition 2 (Key Generation Condition):</u>

A shared key K_{ij} can be determined from the secret key s_i of entity i and the public key v_j of entity j using a key-generation function g (·) ("second function").

$$K_{ij} = g\ (s_i,\ v_j)$$

<u>Condition 3 (Key Sharing Condition):</u>

The shared key K_{ij}, which entity i generates for entity j, and the shared key K_{ji}, which entity j generates for entity i, are alike.

$$K_{ij} = K_{ji}$$

Therefore, a key-sharing function F (·) ("third function"), which can be produced by substituting the secret-key function f (·) for the key-generation function f (·), and which has public keys v_i, v_j as variables, is a symmetric function.

$$F\ (v_i,\ v_j) = F\ (v_j,\ v_i)$$

provided that

$$F\ (v_i,\ v_j) = g\ (f\ (v_i),\ v_j) = g\ (s_i,\ v_j)$$

Further, to construct an ID-NIKS that is secure against a collusion attack by a plurality of entities, the following conditions 4-6 should be satisfied.

<u>Condition 4 (Secret Key Security Against Collusion):</u>

The secret-key function f (·) is a non-separable function as shown below.

$$f\ (x + y) \neq f\ (x)\ \text{O}\ f\ (y)$$

When the secret-key function f (·) is a separable function, the secret key s_z of another entity z can be revealed and generated by a collusion attack using the secret keys s_i, s_j of 2 entities i, j. For example, if $v_z = v_i + v_j$ and secret keys s_i, s_j are prepared in advance, it is possible to determine the secret key s_z of entity z as follows.

$$\begin{aligned} s_z &= f\ (v_z) \\ &= f\ (v_i + v_j) \\ &= f\ (v_i)\ \text{O}\ f\ (v_j) \\ &= s_i\ \text{O}\ s_j \end{aligned}$$

<u>Condition 5 (Shared Key Security Against Collusion):</u>

The key-sharing function F(·), as shown below, is a non-separable function.

$$F\ (a,\ x + y) \neq F\ (a,\ x)\ \text{O}\ F\ (a,\ y)$$

In accordance with Condition 3, since the key-sharing function F(·) is a symmetric function, the following expression is also realized.

$$F\ (x + y,\ a) \neq F\ (x,\ a)\ \text{O}\ F\ (y,\ a)$$

When the key-sharing function F(·) is a separable function,

the shared key may be generated by a collusion attack of entities using a shared key. When entities i, j collude with one another, $v_z = v_i + v_j$, and K_{iy} ($= g(s_i, v_y) = F(v_i, v_y)$) and K_{jy} ($= g(s_j, v_y) = F$ K_{iy} ($= g(s_i, v_y) = F(v_i, v_y)$)) are prepared beforehand, it is possible to determine the shared key K_{yz} between entities y, z as follows.

$$
\begin{aligned}
K_{yz} &= F(v_y, v_z) \\
&= F(v_y, v_i + v_j) \\
&= F(v_y, v_i) \circ F(v_y, v_j) \\
&= F(v_i, v_y) \circ F(v_j, v_y) \\
&= K_{iy} \circ K_{jy}
\end{aligned}
$$

Condition 5 is extremely strict. Regardless of the intermediary calculation, just the fact that the function format in the key sharing stage is separable does not mean that security is perfect. For example, a sum of products-type ID-NIKS, or a power product-type ID-NIKS do not satisfy this condition.

<u>Condition 6 (Security of Center Secrets):</u>

Center secrets cannot be determined no matter what type of attack is perpetrated.

In the present invention, in addition to establishing a third function (key-sharing function) as a non-separable function similar to the prior invention (Condition 5), a first function is established as a non-separable function by treating each entity-specific secret random number as a parameter, and incorporating it into the function (Condition 4). In the present invention, the basis of security is placed on the characteristic of a non-

separable function, and on a difficulty of attack equivalent to RSA cryptography. Further, there is no need to prepare a special prime number in advance, thus heightening freedom of design, and the calculation step for determining a third key (shared key), which both entities share, is completed in one stage, enhancing security and increasing resistance to attack.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a schematic diagram showing the constitution of a cryptographic communication system of the present invention;

Fig. 2 schematically illustrates the state of data communications between 2 entities;

Fig. 3 shows the internal constitution of the shared key generator of Fig. 2;

Fig. 4 is a diagram illustrating the security of secrets at a center when a personal random number is not provided;

Fig. 5 illustrates the security of secrets at a center when a personal random number is provided;

Fig. 6 illustrates a numerical example, which represents the security of the present invention;

Figs. 7A, 7B, 7C, 8A and 8B illustrate in combination a first numerical example according to the present invention;

Figs. 9A, 9B, 9C, 10, 11 and 12 are diagrams showing in combination a second numerical example of the present invention; and

Fig. 13 is a block diagram of the principle of an ID-NIKS

system.

DETAILED DESCRIPTION OF THE INVENTION

Referring to Fig. 1, illustrated is a schematic diagram showing the constitution of a cryptographic communication system according to the present invention. A center 1, which can be trusted to maintain the confidentiality of information, is established. This center 1 may be a public institution. This center 1 is connected to each of a plurality of entities a, b, ..., z, the users, who utilize this cryptographic system, via secret communication channels 2a, 2b, ..., 2z, and secret key data is transmitted to each entity a, b, ..., z from the center 1 via these secret communication channels 2a, 2b, ..., 2z. Further, communication channels 3ab, 3az, 3bz, ... are provided between 2 entities, and a ciphertext, which is encrypted communication information, is transmitted between the entities via this communication channel 3ab, 3az, 3bz, ...

The configuration for implementing the ID-NIKS of the present invention is described hereinbelow. First, the cryptographic system of the present invention is described with respect to "Center 1 Preparations", "Entity Registration", and "Generation of Shared Key Between Entities" in turn.

Center 1 Preparations

The center 1 prepares the following public keys and secret keys, and reveals the public keys.

Public Key	N	N = PQ
	e	Relatively small integer relatively prime to L
Secret Key	P, Q	Large primes
	L	L = λ (N)
	g	Maximum generator over N as a modulus
	T	n x n symmetric matrix (Each component is relatively prime to L)
	r_i	Personal secret random number

Provided that λ $(\cdot)$ is the Carmichael function. The hash function h $(\cdot)$ for calculating an n dimension public key vector v ("first key") from entity ID data is made public at the same time. A hash function is a function, which converts a data string to a different data string, and generally is a function, which converts a long data string to a short data string. When this hash function is used to calculate a public key vector v, the sum of all the components is regulated to become e. That is, the expression hereinbelow is realized. Provided that v_{ik} indicates the kth component of vector v_i. More specifically, when a public key vector v is a binary vector, the Schalkwijk algorithm can be utilized, and in general, (n-1) components are determined by the hash value, and the final 1 component is determined so that the sum of the total is e.

$$e = \sum_{k=1}^{n} v_{ik}$$

Entity Registration

The key management center 1, which is requested by entity i to perform registration, carries out the following calculation using a prepared key and a public key vector v_i (=h (ID_i)) of entity i, determines, in order, entity i vector x_i ("first secret key"), vector s_i ("second secret key"), and y_i ("third secret key"), and completes registration by secretly sending the determined vector s_i and y_i to entity i. Vector x_i, which is a personal secret, is not sent directly to entity i at this time.

1. Determine $\vec{x_i}$

$$\vec{x_i} \equiv T^{\vec{v_i}} \pmod{L}$$

2. Select a random number r_i that is relatively prime to L, and determine $\vec{s_i}$

$$\vec{s_i} \equiv r_i \cdot \vec{x_i} \pmod{L}$$

3. Determine r_i^{-e} (mod L), and determine y_i.

$$y_i \equiv g^{r_i^{-e}} \pmod{N}$$

—————— Equation 8

Generation of Inter-entity Shared Key

In order for entity i to share a key with entity j, a shared key K_{ij} ("third key") is determined by repeating e times high-speed exponentiation like the following.

$$\begin{aligned} K_{ij} &\equiv (\cdots((\cdots((\cdots(y_i^{s_{i1}})\overbrace{\cdots)}^{v_{j1}}{}^{s_{i2}})\overbrace{\cdots)}^{v_{j2}}\cdots\overbrace{{}^{s_{in}})\cdots)}^{v_{jn}}{}^{s_{in}} \\ &\equiv y_i^{\overbrace{s_{i1}\cdots s_{i1}}^{v_{j1}}\overbrace{s_{i2}\cdots s_{i2}}^{v_{j2}}\cdots\overbrace{s_{in}\cdots s_{in}}^{v_{jn}}} \\ &\equiv y_i^{{}^t\vec{s_i}\,\vec{v_j}} \end{aligned}$$

$$
\begin{aligned}
&\equiv y_i^{\left(\prod_{k=1}^{n} r_i^{v_{ik}}\right) \cdot {}^t\overrightarrow{x_i}\,\overrightarrow{v_j}} \\
&\equiv y_i^{r_i^{\left(\sum_{k=1}^{n} v_{ik}\right)} \cdot {}^t\overrightarrow{x_i}\,\overrightarrow{v_j}} \\
&\equiv y_i^{r_i^{e} \cdot {}^t\overrightarrow{x_i}\,\overrightarrow{v_j}} \\
&\equiv g^{r_i^{-e} \cdot r_i^{e} \cdot {}^t\overrightarrow{x_i}\,\overrightarrow{v_j}} \\
&\equiv g^{{}^t\overrightarrow{x_i}\,\overrightarrow{v_j}} \\
&\equiv g^{{}^t\overrightarrow{v_i}\,\mathrm{T}\,\overrightarrow{v_j}} \pmod{N} \qquad \text{---- Equation 9}
\end{aligned}
$$

The communication of information between entities in the above-described cryptographic system is described next. Fig. 2 schematically shows data communications between 2 entities a, b. The example of Fig. 2 depicts a situation, in which entity a encrypts a plaintext (message) M into a ciphertext C, and transmits it to entity b, and entity b decrypts this ciphertext C into the original plaintext (message) M.

The entity a side comprises a public key generator 11, which produces a vector v_b (public key) by inputting entity b personal identification data ID_b, and using a hash function; a shared key generator 12, which generates a shared key K_{ab} for between entities a and b that is sought by entity a on the basis of secret vectors s_a and y_a sent from the key managing center or KMC 1, and vector v_b, which is the public key from the public key generator 11; and an encryption unit 13, which uses the shared key K_{ab} to encrypt a plaintext (message) M into a ciphertext C and outputs it to a communication channel 30.

The entity b side comprises a public key generator 21, which produces a vector v_a (public key) by inputting entity a personal

identification data ID_a, and using a hash function; a shared key generator 22, which generates a shared key K_{ba} for communication with entity a that is sought by entity b on the basis of secret vectors s_b and y_b sent from the center 1, and vector v_a, which is the public key from the public key generator 21; and a decryption unit 23, which uses the shared key K_{ba} to decrypt a ciphertext C inputted from a communication channel 30 into a plaintext (message) M and outputs it.

Fig. 3 is a diagram showing the internal constitution of the shared key generator 12 (22) of Fig. 2. The shared key generator 12 (22) has a first register 41, which stores vector s sent from the center 1; a second register 42, which stores each component of vector s; a third register 43, which stores y sent from the center 1; a fourth register 44, which stores vector v sent from the public key generator 11 (21); a fifth register 45, which stores each component of vector v; a sixth register 46, which stores a natural number N; and a highspeed exponent computing element 47, which uses the outputs of the second, third, fifth and sixth registers 42, 43, 45, 46 to perform the exponentiation shown in Equation 9.

The operation is described next. When entity a attempts to send information to entity b, first of all, the personal identification data ID_b of entity b is inputted to the public key generator 11, vector v_b (public key) is produced, and the produced vector v_b is sent to the shared key generator 12. Further, vectors s_a and y_a, which are determined by the center 1 in accordance with Equation 8, are inputted to the shared key generator 12. A shared key K_{ab} is determined in accordance with

Equation 9 by the shared key generator 12 of Fig. 3, and sent to the encryption unit 13. In the encryption unit 13, a plaintext (message) M is encrypted into a ciphertext C using this shared key K_{ab}, and the ciphertext C is transmitted via the communication channel 30.

The ciphertext C transmitted over the communication channel 30 is inputted to the decryption unit 23 of entity b. The personal identification data ID_a of entity a is inputted to the public key generator 21, vector v_a (public key) is produced, and the produced vector v_a is sent to the shared key generator 22. Further, the vectors x_b and y_b, which are determined by the center 1 in accordance with Equation 8, are inputted to the shared key generator 22. A shared key K_{ba} is determined in accordance with Equation 9 by the shared key generator 22 of Fig. 3, and sent to the decryption unit 23. In the decryption unit 23, the ciphertext C is decrypted into a plaintext (message) M using this shared key K_{ba}.

Next, verification is made of the fact that this cryptographic system of the present invention satisfies the above-described ID-NIKS achievability (Conditions 1-3) and ID-NIKS security (Conditions 4-6).

<u>For Condition 1</u>

The secret-key function f $(\cdot)$ is defined as shown below having a personal secret random number r_i as a parameter, and using this secret-key function f $(\cdot)$, the center 1 can determine a corresponding secret key from the public key of an entity.

$$f_{r_i}(\vec{v_i}) \equiv r_i \mathrm{T}^{\vec{v_i}} \pmod{L}$$

(For Condition 2)

The key-generation function g (·) is defined as shown below, and a shared key can be generated from the secret key of one entity and the public key of another entity.

$$\mathcal{G}(\{y_i, \vec{s_i}\}, \vec{v_j}) \equiv y_i^{{}^t\vec{s_i}\,\vec{v_j}} \pmod{N}$$

For Condition 3

The key-sharing function F (·) is defined by the following expression, and since a center secret matrix T is a symmetric matrix, F (·) is a symmetric function as shown in the following expression, and shared keys generated by reciprocal entities are identical.

$$\mathcal{F}(\vec{v_i}, \vec{v_j}) \equiv g^{{}^t\vec{v_i}\,\mathrm{T}\,\vec{v_j}} \pmod{N}$$

$$\begin{aligned} \mathcal{F}(\vec{x}, \vec{y}) &= g^{{}^t\vec{x}\,\mathrm{T}\,\vec{y}} \\ &= g^{{}^t\vec{y}\,{}^t\mathrm{T}\,\vec{x}} \\ &= \mathcal{F}(\vec{y}, \vec{x}) \end{aligned}$$

For Condition 4

The secret-key function f (·), as shown below, constitutes a separable function when parameter r is fixed, but since the value of this parameter r is different for each entity in the

cryptographic system of the present invention, the secret-key function f (·) is a non-separable function.

$$
\begin{aligned}
f_r(\vec{x}+\vec{y}) &= r\mathbf{T}^{\vec{x}+\vec{y}} \\
&= r(\mathbf{T}^{\vec{x}} * \mathbf{T}^{\vec{y}}) \\
&= r\mathbf{T}^{\vec{x}} * r\mathbf{T}^{\vec{y}} \\
&= f_r(\vec{x}) * f_r(\vec{y})
\end{aligned}
$$

For example, when vector $v_x \equiv$ vector v_i + vector v_j, then vector $x_x \equiv$ vector x_i * vector x_j, but because vector x_i itself is not distributed to an entity, and vector s_i, which multiplies a personal random number r_i thereby, is distributed, vector $s_x \equiv$ vector s_i * vector s_j is not realized, and neither vector s_x nor vector x_x, which are personal secrets, can be determined.

<u>For Condition 5</u>

Because the key-sharing function F (·) is a non-separable function, as shown in the following expression, no matter how many public keys and secret keys are gathered in accordance with the collusion of a plurality of entities, the keys shared between any other entities cannot be determined.

$$
\begin{aligned}
\mathcal{F}(\vec{a}, \vec{x}+\vec{y}) &= g^{{}^t\vec{a}\mathbf{T}^{\vec{x}+\vec{y}}} \\
&= g^{{}^t\vec{a}\mathbf{T}^{\vec{x}} \cdot {}^t\vec{a}\mathbf{T}^{\vec{y}}} \\
&\neq \mathcal{F}(\vec{a}, \vec{x}) \circ \mathcal{F}(\vec{a}, \vec{y})
\end{aligned}
$$

<u>For Condition 6</u>

Center secrets (P, Q, L, g, r_i, and T) are not revealed even when a plurality of entities collude with one another. The bases for center secrets P, Q, L, g, and r_i not being revealed are as follows.

P, Q, L: Difficulty of factorization of N

g: Security in accordance with r_i being unknown

r_i: Difficulty of a discrete logarithm problem over a composite number as a modulus

Next, the security of the center secret matrix T is considered. Here, the security of the center secret matrix T is considered with regard to an attack, in which colluding entities attempt to solve a high-order linear congruence expression by pooling their individual private keys.

In the cryptographic system of the present invention, an attack must be performed considering that the personal random number is also a center secret variable, in addition to the n (n + 1)/2 center secret variables of the center secret matrix T. For example, when m entities are in collusion, the number of the center secret variables is {n (n + 1)/2 + m}. As a result thereof, even if an arbitrary number of entities collude with one another, it is impossible to generate the center secret matrix T. The reason this is impossible is described hereinbelow for each possible number of colluding entities.

<u>When less than n entities are in collusion</u>

Because the number of center secret variables exceeds the number of linearly-independent expressions obtained in accordance with collusion, the center secret matrix T cannot be generated.

When n entities are in collusion

When n entities are in collusion, a maximum of {n (n + 1)/2 + (n − 1)} linearly-independent expressions can be obtained. In the meantime, since there are {n (n + 1)/2 + n} center secret variables, the number of linearly-independent expressions is 1 fewer than the number of center secret variables, making it impossible to generate/break the center secret matrix T.

When (n + 1) entities are in collusion

Compared to when n entities are colluding, 1 personal secret random number is newly added, but other n items are linearly subordinate so that only 1 new linearly-independent expression can be obtained. Thus, there is an increase of only 1 linearly-independent expression when the center secret variables are increased by 1. Accordingly, if the center secret matrix T cannot be solved when n entities collude, it cannot be solved when (n + 1) entities collude, either.

From the above, even if (n + 2) or more entities collude with one another, since the number of congruence expressions will, inductively, always be 1 or more fewer than the number of unknown variables, the indeterminateness of the solution cannot be removed. Further, the above-described simultaneous congruence expression is generally a high-order simultaneous congruence expression so that the solution is difficult. Furthermore, ultimately, an operation, which multiplies an inverse element that has L as a modulus, is absolutely necessary. For an attacker, who does not know modulus L, this is tantamount to breaking RSA cryptography.

Further, let's assume, hypothetically, that, without solving

for the equation, it is possible to eliminate one variable by using the fact that the number of congruence expressions is one fewer than the number of unknown variables. In this case, a linear attack can be utilized, but because the vector v_x of the target entity is a fixed-weight vector, a negative coefficient is absolutely necessary to express it using a linear association of other entities (or another entity), so that, in this case as well, for an attacker, who does not know modulus L, it is equivalent to breaking RSA cryptography.

As described above, the center secret matrix T can be said to be secure against a collusion attack in the cryptographic system of the present invention.

Specific examples of the security of the center secret matrix T are described hereinbelow when a personal random number is provided, and when a personal random number is not provided. Fig. 4 depicts a situation, in which a personal random number is not provided, and 5 entities are in collusion. As illustrated in Fig. 4, since a 5 x 5 matrix T is a symmetric matrix, the unknown quantity of components is 15. Further, as illustrated in the drawing, the number of linearly-independent expressions is 5 + 4 + 3 + 2 + 1 = 15. Accordingly, the number of unknown quantities and the number of linearly-independent expressions match so that the equation can be solved, and the center secret matrix T can be determined.

Conversely, Fig. 5 depicts a situation, in which a personal random number is provided, and 5 entities collude with one another. Because the personal random number is also a center 1

secret, the unknown quantity is 15 components derived from the matrix T and 5 components derived from the random numbers for a total of 20. Further, as illustrated in Fig. 5, the number of linearly-independent expressions is 5 + 5 + 4 + 3 + 2 = 19. Accordingly, the number of unknown quantities is larger than the number of linearly-independent expressions so that a solution is not possible, and center 1 secrets cannot be determined. Fig. 6 shows the equation in the case thereof.

Next, numerical examples of the cryptographic communication method of the present invention are described. A first numerical example (when the public key vector v components are binary, and 2 entities i, j share keys) is illustrated in Figs. 7A, 7B, 7C, 8A and 8B. First, as shown in Fig. 7A, public keys (N, e) and secret keys (P, Q, L, g, T, r_i, r_j) are set in the center 1. Further, binary public key vectors v_i, v_j are calculated based on the ID of each entity i, j, and arranged as shown in Fig. 7B. When the r_i^{-e}, r_j^{-e} of each entity i, j is determined based on the above setting conditions, the results are like those illustrated in Fig. 7C. Furthermore, when vectors s_i, y_i, and shared key K_{ij} of entity i are determined, the results are as depicted in Fig. 8A, and similarly, when vectors s_j, y_j, and shared key K_{ji} of entity j are determined, the results are as depicted in Fig. 8B.

Figs. 9A-Fig. 12 depict a second numerical example (when the public key vector v components are multiple notation values (e.g. ternary or decimal), and 3 entities i, j, k share keys). First, as illustrated in Fig. 9A, public keys (N, e) and secret keys (P, Q, L, g, T, r_i, r_j, r_k) are set in the center 1. Further, multi-

notation public key vectors v_i, v_j, v_k are calculated based on the ID of each entity i, j, k, and set as shown in Fig. 9B. When the r_i^{-e}, r_j^{-e}, r_k^{-e}, and vectors s_i, s_j, s_k, and y_i, y_j, y_k of each entity i, j, k are determined based on the above setting conditions. The results are illustrated in Fig. 9C. Then, the shared key $K_{ij} = K_{ji}$ between entities i, j, the shared key $K_{ik} = K_{ki}$ between entities i, k, and the shared key $K_{jk} = K_{kj}$ between entities j, k, respectively, are determined as illustrated in Figs. 10, 11, and 12.

As understood from the foregoing, since the above-described 3 conditions for achieving ID-NIKS, and the 3 conditions for ensuring the security thereof are both satisfied in the present invention, center secret parameters are not revealed, and a ciphertext cannot be decrypted, no matter how many entities collude. The present invention therefore achieves extremely high security in ID-NIKS.

Further, there is no need to prepare a special pattern of prime numbers in advance unlike the prior invention (JP A-10-210022), thus enhancing the freedom of design, and the key sharing procedure can be accomplished in a one-stage calculation step, thus improving security against attack as compared with the prior invention.

This application claims priority of Japanese Patent Application Serial No. 10-125086 filed May 7, 1998 and the entire disclosure thereof is incorporated herein by reference.

CLAIMS

What Is Claimed Is:

1. A cryptographic communication method for communication of information from one entity to another entity, using publicly available each entity-specific public first keys of the one and another entities, comprising:

causing a center to prepare each entity-specific secret second keys based on each entity-specific public first keys using a first function and to send the each entity-specific secret second keys to the one and another entities respectively, the first function having as parameters each entity-specific random numbers controlled by the center;

preparing a third key which is expressed as a second function having 2 variables, i.e., the one entity's second key and another entity's first key, or the another entity's second key and one entity's first key, the third key being shared by the one and another entities;

causing one entity to encrypt a plaintext into a ciphertext by using the third key and to transmit it to the another entity; and

causing the another entity to decrypt the ciphertext into the original plaintext by using the third key, and

wherein the first function, and a third function which is obtained by substituting the first function for the second function and which has the one entity's and another entity's

first keys as variables, are set in the below defined non-separable function for each respective variable.

Definition: When a suitable commutative operation is treated as O and function $f(\cdot)$ satisfies $f(x + y) \neq f(x) \text{ O } f(y)$, the function $f(\cdot)$ is non-separable in accordance with the operation O.

2. The cryptographic communication method according to claim 1, wherein each of said second keys comprises a first secret key, which is generated from the each entity-specific first key and a symmetric matrix controlled by said center; a second secret key, which is generated by multiplying a random number by the first secret key; and a third secret key, which is generated on the basis of the random number, said center sends the second and third secret keys to each entity, and the one entity generates the third key using the second and third secret keys and the first key of the another entity.

3. The cryptographic communication method according to claim 2, wherein a below shown arithmetic expression is utilized when said center generates the first, second and third secret keys.

$$\vec{x_i} \equiv \mathbf{T}^{\vec{v_i}} \pmod{L}$$

$$\vec{s_i} \equiv r_i \cdot \vec{x_i} \pmod{L}$$

$$y_i \equiv g^{r_i^{-e}} \pmod{N}$$

Provided that

Vector v_i: First key of entity i

Vector x_i: First secret key of entity i

Vector s_i: Second secret key of entity i

y_i: Third secret key of entity i

r_i: Random number of entity i

L: $L = \lambda\ (N)$

N: N = PQ (P, Q are prime numbers)

T: Symmetric matrix (Each component being relatively prime to L)

g: Maximum generator over N as a modulus

e: an integer that is relatively prime to L

$\lambda\ (\cdot)$: Carmichael function

4. The cryptographic communication method according to claim 3, wherein a below shown arithmetic expression is utilized when the one entity generates the third key based on the second and third secret keys and the first key of the another entity.

$$
\begin{aligned}
K_{ij} &\equiv (\cdots((\cdots((\cdots(y_i^{\overbrace{s_{i1})\cdots)}^{v_{j1}}\overbrace{{}^{s_{i2}})\cdots)}^{v_{j2}}\cdots\overbrace{{}^{s_{in}})\cdots)^{s_{in}}}^{v_{jn}} \\
&\equiv y_i^{\overbrace{s_{i1}\cdots s_{i1}}^{v_{j1}}\overbrace{s_{i2}\cdots s_{i2}}^{v_{j2}}\cdots\overbrace{s_{in}\cdots s_{in}}^{v_{jn}}} \\
&\equiv y_i^{{}^t\overrightarrow{s_i}\overrightarrow{v_j}} \\
&\equiv y_i^{\left(\prod_{k=1}^{n} r_i^{v_{ik}}\right)\cdot{}^t\overrightarrow{x_i}\overrightarrow{v_j}} \\
&\equiv y_i^{r_i^{\left(\sum_{k=1}^{n} v_{ik}\right)}\cdot{}^t\overrightarrow{x_i}\overrightarrow{v_j}} \\
&\equiv y_i^{r_i^{e}\cdot{}^t\overrightarrow{x_i}\overrightarrow{v_j}} \\
&\equiv g^{r_i^{-e}\cdot r_i^{e}\cdot{}^t\overrightarrow{x_i}\overrightarrow{v_j}} \\
&\equiv g^{{}^t\overrightarrow{x_i}\overrightarrow{v_j}} \\
&\equiv g^{{}^t\overrightarrow{v_i}\mathrm{T}\overrightarrow{v_j}} \pmod{N}
\end{aligned}
$$

5. The cryptographic communication method according to claim 1, wherein the each entity-specific first key is determined by calculating identification information of each entity using a hash function.

6. The cryptographic communication method according to claim 2, wherein the each entity-specific first key is determined by calculating identification information of each entity using a hash function.

7. The cryptographic communication method according to claim 3, wherein the each entity-specific first key is determined by calculating identification information of each entity using a hash function.

8. The cryptographic communication method according to claim 4, wherein the each entity-specific first key is determined by calculating identification information of each entity using a hash function.

9. An encryption method to be used by one entity when the one entity encrypts a plaintext to a ciphertext and sends it to another entity, using publicly available each entity-specific public first keys of the one and another entities, comprising:

causing a center to prepare an entity-specific secret second key for the one entity based on the one entity's public first key using a first function and to send the entity-specific secret second key to the one entity, the first function having as parameters each entity-specific random numbers controlled by the center;

preparing a third key, which is expressed by a second function having 2 variables (i.e., the secret second key of the one entity and the public first key of the another entity); and

causing the one entity to encrypt a plaintext into a ciphertext by using the third key, and

wherein the first function, and a third function, which is obtained by substituting the first function for the second function, and which has the one entity's and the another entity's first keys as variables, are set in the below-defined non-separable function for each respective variable.

Definition: When a suitable commutative operation is treated as O and function $f(\cdot)$ satisfies $f(x + y) \neq f(x)\ \mathrm{O}\ f(y)$, the function $f(\cdot)$ is non-separable in accordance with the operation O.

10. A cryptographic communication system using publicly available each entity-specific public first keys, comprising:

a center, which prepares and sends an each entity-specific secret second key to each entity, the center preparing the each entity-specific secret second keys from each entity-specific public first keys using a first function, the first function having as parameters each entity-specific random numbers controlled by the center; and

a plurality of entities, one entity of which encrypts a plaintext into a ciphertext using a third key and transmits it to another entity among the plurality of entities, and the another entity of which receives the ciphertext decrypts the ciphertext into the original plaintext using the third key, the one and another entities determining the mutual third key that is expressed by a second function in accordance with 2 variables (i.e., the second key of the one entity and the first key of the another entity, or the second key of the another entity and the first key of the one entity), and

wherein the first function, and a third function, which is obtained by substituting the first function for the second function, and which has the one entity's and the another entity's first keys as variables, are set in the below defined non-separable function for each respective variable.

Definition: When a suitable commutative operation is treated as O and function $f(\cdot)$ satisfies $f(x + y) \neq f(x) \mathrm{O} f(y)$, the function $f(\cdot)$ is non-separable in accordance with the operation O.

11. The cryptographic communication system according to claim 10, wherein each of said second keys comprises a first secret key, a second secret key, and a third secret key, and said center comprises means for calculating the first secret key from each entity-specific first key and a symmetric matrix controlled by said center, means for calculating the second secret key by multiplying the first secret key by a random number and means for calculating the third secret key on the basis of the random number, and sends the calculated second and third secret keys to each entity.

12. The cryptographic communication system according to claim 11, wherein each of said entities includes means for calculating the third key from the second and third secret keys sent from the center and the first key of the communicating entity.

CRYPTOGRAPHIC COMMUNICATION METHOD AND ENCRYPTION METHOD AND CRYPTOGRAPHIC COMMUNICATION SYSTEM

ABSTRACT OF THE DISCLOSURE

A method for cryptographic communication between two entities. A center prepares each entity-specific secret second keys based on publicly available each entity-specific public first keys using a first function and sends the each entity-specific secret second keys to the two entities respectively. The first function has as parameters each entity-specific random numbers controlled by the center. A third key is prepared which is expressed as a second function having 2 variables, i.e., one entity's second key and another entity's first key, or another entity's second key and one entity's first key. The third key is shared by the two entities. The one entity encrypts a plain-text into a ciphertext by using the third key and to transmit it to another entity. Another entity decrypts the ciphertext into the original plaintext by also using the third key. The first function, and a third function which is obtained by substituting the first function for the second function and which has the one entity's and another entity's first keys as variables, are set in the below defined non-separable function for each respective variable. Definition: When a suitable commutative operation is treated as $\bigcirc$ and function $f(\cdot)$ satisfies $f(x + y) \neq f(x) \bigcirc f(y)$, the function $f(\cdot)$ is non-separable in accordance with the operation $\bigcirc$.

FIG. 1

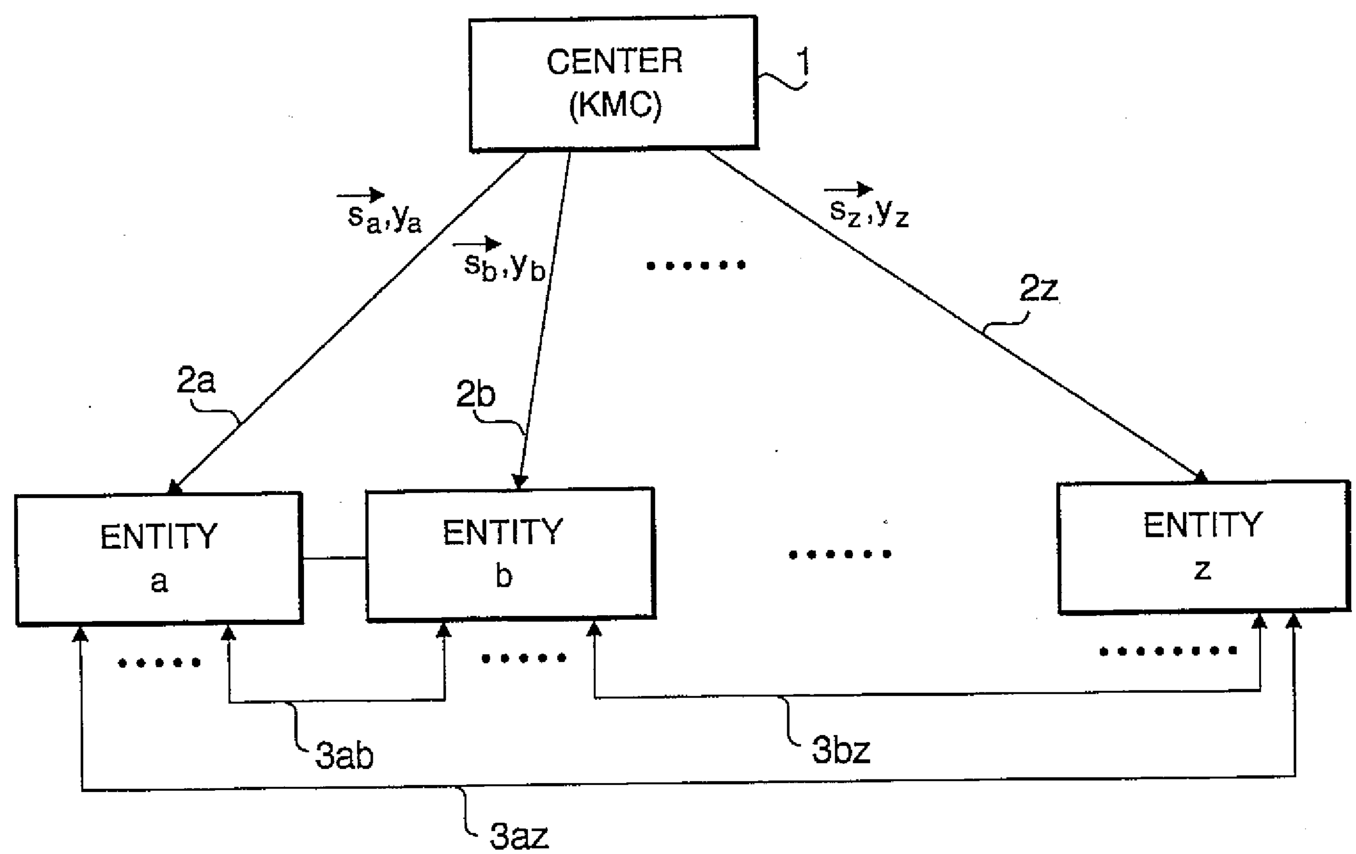

CENTER
(KMC)
1
$\vec{s}_a, y_a$
$\vec{s}_b, y_b$
$\vec{s}_z, y_z$
2a
2b
2z
ENTITY
a
ENTITY
b
ENTITY
z
3ab
3bz
3az

FIG. 2

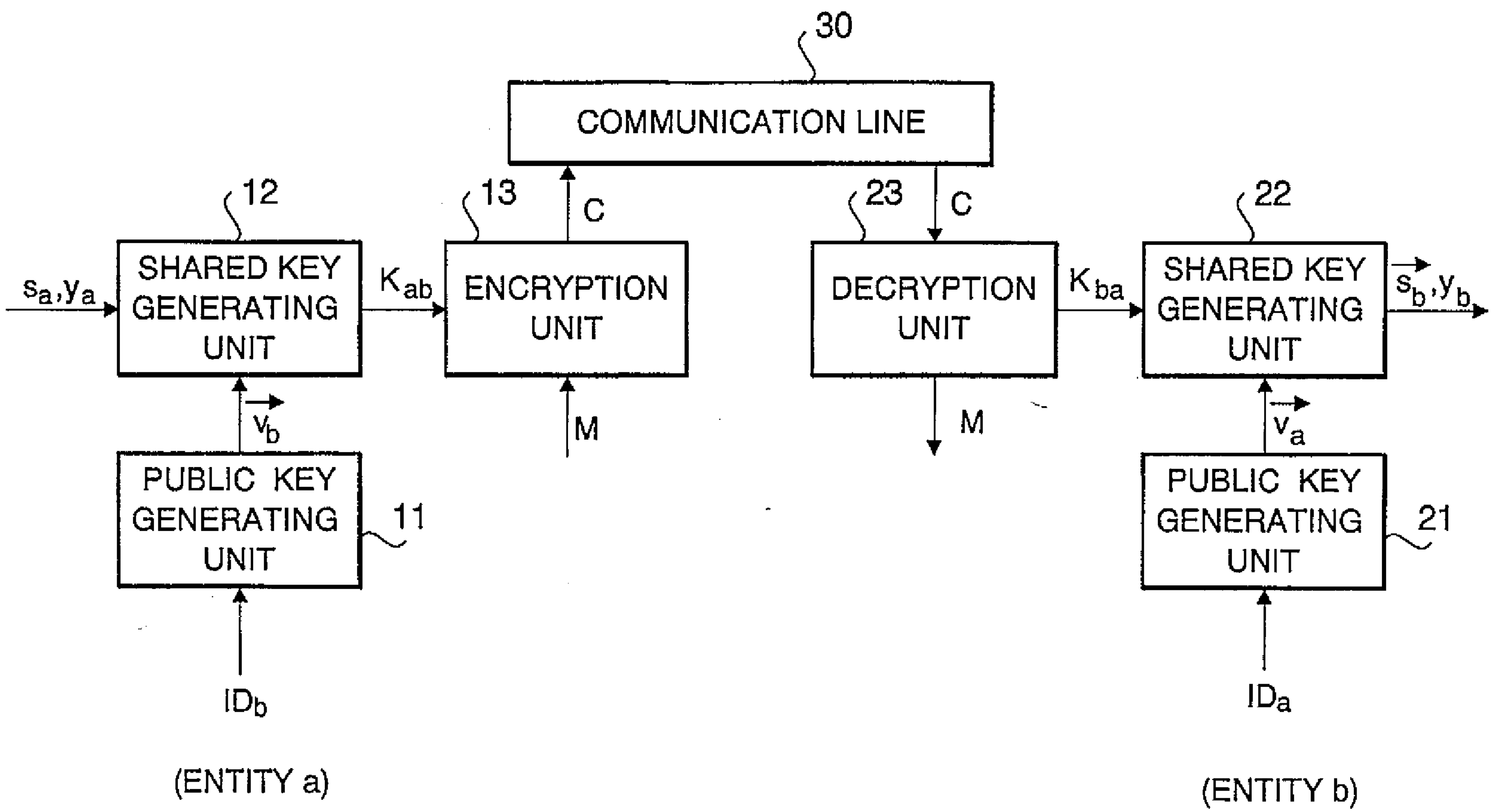
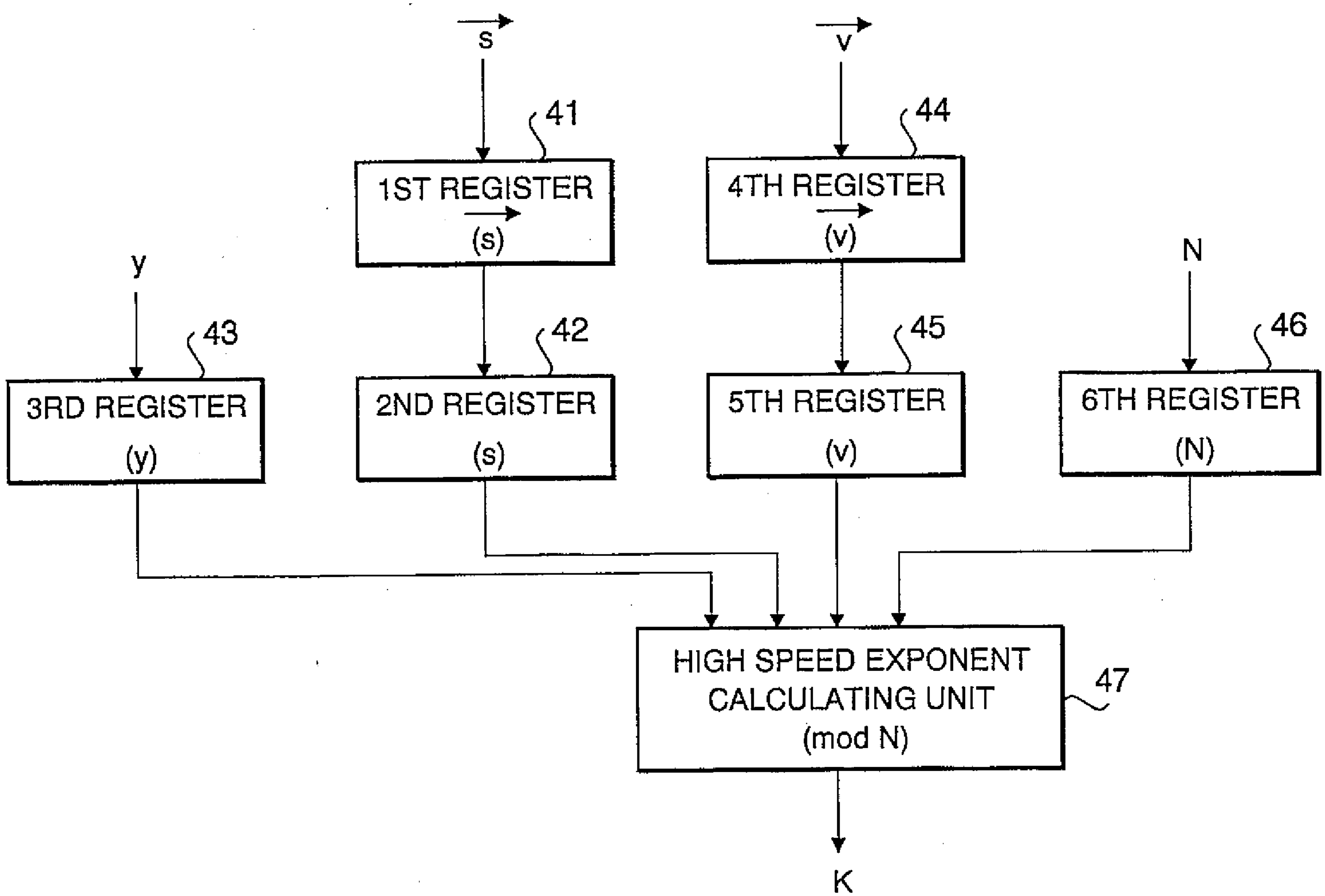

30
COMMUNICATION LINE
12
SHARED KEY GENERATING UNIT
13
ENCRYPTION UNIT
23
DECRYPTION UNIT
22
SHARED KEY GENERATING UNIT
s_a, y_a
K_{ab}
C
C
K_{ba}
$\vec{s_b}, y_b$
$\vec{v_b}$
M
M
$\vec{v_a}$
PUBLIC KEY GENERATING UNIT
11
PUBLIC KEY GENERATING UNIT
21
ID_b
ID_a
(ENTITY a)
(ENTITY b)

FIG. 3



s
41
1ST REGISTER
(s)
v
44
4TH REGISTER
(v)
y
43
3RD REGISTER
(y)
42
2ND REGISTER
(s)
45
5TH REGISTER
(v)
N
46
6TH REGISTER
(N)
HIGH SPEED EXPONENT
CALCULATING UNIT
(mod N)
47
K

FIG. 4

$$T = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ a_2 & b_1 & b_2 & b_3 & b_4 \\ a_3 & b_2 & c_1 & c_2 & c_3 \\ a_4 & b_3 & c_2 & d_1 & d_2 \\ a_5 & b_4 & c_3 & d_2 & e_1 \end{pmatrix}$$

15 UNKNOWN ELEMENTS

$$\vec{v}_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \quad \vec{v}_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \quad \vec{v}_3 = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \quad \vec{v}_4 = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \quad \vec{v}_5 = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

$$\vec{x}_i = T\vec{v}_i$$

$$\vec{x}_1 = \begin{pmatrix} a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \end{pmatrix} \Big\} 5 \qquad \vec{x}_3 = \begin{pmatrix} a_3 \\ b_2 \\ c_1 \\ c_2 \\ c_3 \end{pmatrix} \Big\} 3 \qquad \vec{x}_5 = \begin{pmatrix} a_5 \\ b_4 \\ c_3 \\ d_2 \\ e_1 \end{pmatrix} \Big\} 1$$

$$\vec{x}_2 = \begin{pmatrix} a_2 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \end{pmatrix} \Big\} 4 \qquad \vec{x}_4 = \begin{pmatrix} a_4 \\ b_3 \\ c_2 \\ d_1 \\ d_2 \end{pmatrix} \Big\} 2$$

INDEPENDENT LINEAR EXPRESSIONS = 5+4+3+2+1=15

NO. OF UNKNOWN ELEMENTS : 15 = NO. OF INDEPENDENT LINER EXPRESSIONS : 15

⇩

CAN BE SOLVED

FIG. 5

SECRET MATRIX OF CENTER

$$T' = [T|R] = \left(\begin{array}{ccccc|ccccc} a_1 & a_2 & a_3 & a_4 & a_5 & r_1 & r_2 & r_3 & r_4 & r_5 \\ a_2 & b_1 & b_2 & b_3 & b_4 & r_1 & r_2 & r_3 & r_4 & r_5 \\ a_3 & b_2 & c_1 & c_2 & c_3 & r_1 & r_2 & r_3 & r_4 & r_5 \\ a_4 & b_3 & c_2 & d_1 & d_2 & r_1 & r_2 & r_3 & r_4 & r_5 \\ a_5 & b_4 & c_3 & d_2 & e_1 & r_1 & r_2 & r_3 & r_4 & r_5 \end{array}\right)$$

20 UNKNOWN ELEMENTS

ENTITY PUBLIC VECTORS CORRESPONDING TO T'

$$\vec{v}_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \quad \vec{v}_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \quad \vec{v}_3 = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \quad \vec{v}_4 = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \quad \vec{v}_5 = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

$$\vec{s}_i = r_i\, T\vec{v}_i$$

$$\vec{s}_1 = \begin{pmatrix} a_1 r_1 \\ a_2 r_1 \\ a_3 r_1 \\ a_4 r_1 \\ a_5 r_1 \end{pmatrix} \Big\}\,5 \qquad \vec{s}_3 = \begin{pmatrix} a_3 r_3 \\ b_2 r_3 \\ c_1 r_3 \\ c_2 r_3 \\ c_3 r_3 \end{pmatrix} \Big\}\,4 \qquad \vec{s}_5 = \begin{pmatrix} a_5 r_5 \\ b_4 r_5 \\ c_3 r_5 \\ d_2 r_5 \\ e_1 r_5 \end{pmatrix} \Big\}\,2$$

$$\vec{s}_2 = \begin{pmatrix} a_2 r_2 \\ b_1 r_2 \\ b_2 r_2 \\ b_3 r_2 \\ b_4 r_2 \end{pmatrix} \Big\}\,5 \qquad \vec{s}_4 = \begin{pmatrix} a_4 r_4 \\ b_3 r_4 \\ c_2 r_4 \\ d_1 r_4 \\ d_2 r_4 \end{pmatrix} \Big\}\,3$$

INDEPENDENT LINEAR EXPRESSIONS = 5+5+4+3+2=19

NO. OF UNKNOWN ELEMENTS : 20 > NO. OF INDEPENDENT LINER EXPRESSIONS : 19

⇩

CANNOT BE SOLVED

FIG. 6

$$
\begin{pmatrix}
x_1[1]\\ x_1[2]\\ x_1[3]\\ x_1[4]\\ x_1[5]\\
x_2[1]\\ x_2[2]\\ x_2[3]\\ x_2[4]\\ x_2[5]\\
x_3[1]\\ x_3[2]\\ x_3[3]\\ x_3[4]\\ x_3[5]\\
x_4[1]\\ x_4[2]\\ x_4[3]\\ x_4[4]\\ x_4[5]\\
x_5[1]\\ x_5[2]\\ x_5[3]\\ x_5[4]\\ x_5[5]
\end{pmatrix}
=
\begin{pmatrix}
1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0\\
0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0\\
0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0\\
0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0\\
0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0\\
0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0\\
0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&1&0&0&0\\
0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&1&0&0&0\\
0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&1&0&0&0\\
0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&1&0&0&0\\
0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0\\
0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&1&0&0\\
0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&1&0&0\\
0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&1&0&0\\
0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&1&0&0\\
0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0\\
0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&1&0\\
0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&1&0\\
0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&1&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&1&0\\
0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1\\
0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&1\\
0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&1
\end{pmatrix}
\begin{pmatrix}
a_1\\ a_2\\ a_3\\ a_4\\ a_5\\
b_1\\ b_2\\ b_3\\ b_4\\
c_1\\ c_2\\ c_3\\
d_1\\ d_2\\
e_1\\
r'_1\\ r'_2\\ r'_3\\ r'_4\\ r'_5
\end{pmatrix}
$$

FIG. 7A

$P=47,\ Q=59$
$N=2773,\ L=1334$
$g=2449,\ e=5$
$r_i=673,\ r_j=239$

$$T=\begin{pmatrix} 547 & 416 & 360 & 309 & 339 & 288 & 396 & 470 \\ 416 & 359 & 303 & 252 & 280 & 210 & 341 & 409 \\ 360 & 303 & 241 & 194 & 224 & 173 & 288 & 351 \\ 309 & 252 & 194 & 139 & 173 & 120 & 234 & 178 \\ 339 & 280 & 224 & 173 & 197 & 148 & 262 & 331 \\ 288 & 210 & 173 & 120 & 148 & 101 & 210 & 275 \\ 396 & 341 & 288 & 234 & 262 & 210 & 331 & 393 \\ 470 & 409 & 351 & 178 & 331 & 275 & 393 & 457 \end{pmatrix}$$

FIG. 7B

$$\vec{v_i}=\begin{pmatrix}1\\0\\1\\0\\1\\1\\0\\1\end{pmatrix},\quad \vec{v_j}=\begin{pmatrix}0\\1\\1\\1\\0\\1\\1\\0\end{pmatrix}$$

FIG. 7C

$r_i^{-e}=863$

$r_j=49$

FIG. 8A

ENTITY i

$$\vec{s_i} = \begin{pmatrix} 390 \\ 340 \\ 994 \\ 292 \\ 1054 \\ 1314 \\ 1086 \\ 244 \end{pmatrix} \quad \vec{v_j} = \begin{pmatrix} 0 \\ 1 \\ 1 \\ 1 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix}, \quad y_i = 1721$$

$$K_{ij} = \left(\left(\left(\left(1721^{340}\right)^{994}\right)^{292}\right)^{1314}\right)^{1086} = 51 \ (\mathrm{mod}\, 2773)$$

FIG. 8B

ENTITY j

$$\vec{s_j} = \begin{pmatrix} 954 \\ 206 \\ 1266 \\ 914 \\ 814 \\ 454 \\ 862 \\ 72 \end{pmatrix} \quad \vec{v_i} = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 1 \\ 1 \\ 0 \\ 1 \end{pmatrix}, \quad y_j = 689$$

$$K_{ji} = \left(\left(\left(\left(689^{954}\right)^{1266}\right)^{814}\right)^{454}\right)^{72} = 51 \ (\mathrm{mod}\, 2773)$$

FIG. 9A

$P=47,\ Q=59$
$N=2773,\ L=1334$
$g=2449,\ e=17$
$r_i=113,\ r_j=327,\ r_k=295$

$$T=\begin{pmatrix} 852 & 221 & 738 \\ 221 & 253 & 846 \\ 738 & 846 & 785 \end{pmatrix}$$

FIG. 9B

$$\vec{v_i}=\begin{pmatrix} 3 \\ 5 \\ 9 \end{pmatrix},\quad \vec{v_j}=\begin{pmatrix} 4 \\ 11 \\ 2 \end{pmatrix},\quad \vec{v_k}=\begin{pmatrix} 6 \\ 3 \\ 8 \end{pmatrix}$$

FIG. 9C

$r_i^{-e}=681,\ r_j^{-e}=641,\ r_k^{-e}=1115,$

$$\vec{s_i}=\begin{pmatrix} 878 \\ 276 \\ 194 \end{pmatrix},\ \vec{s_j}=\begin{pmatrix} 256 \\ 138 \\ 76 \end{pmatrix},\ \vec{s_k}=\begin{pmatrix} 652 \\ 1288 \\ 778 \end{pmatrix}$$

$y_i=2088,\ y_j=1689,\ y_k=13$

FIG. 10

$$K_{ij} = K_{ji}$$

$$K_{ij} = \left(\left(2088^{878^{4}} \right)^{276^{11}} \right)^{194^{2}}$$

$$= \left(\left(\left(\left(\left(\left(\left(\left(\left(\left(\left(\left(\left(\left(\left(\left(\left(2088^{878}\right)^{878}\right)^{878}\right)^{878}\right)^{276}\right)^{276}\right)^{276}\right)^{276}\right)^{276}\right)^{276}\right)^{276}\right)^{276}\right)^{276}\right)^{276}\right)^{276}\right)^{194}\right)^{194}$$

$$= 189 \pmod{2773}$$

$$K_{ji} = \left(\left(1689^{256^{3}} \right)^{138^{5}} \right)^{76^{9}}$$

$$= \left(\left(\left(\left(\left(\left(\left(\left(\left(\left(\left(\left(\left(\left(\left(\left(\left(1689^{256}\right)^{256}\right)^{256}\right)^{138}\right)^{138}\right)^{138}\right)^{138}\right)^{138}\right)^{76}\right)^{76}\right)^{76}\right)^{76}\right)^{76}\right)^{76}\right)^{76}\right)^{76}\right)^{76}$$

$$= 189 \pmod{2773}$$

FIG. 11

$$K_{ik} = K_{ki}$$

$$K_{ik} = \left(\left(2088^{878^{6}}\right)^{276^{3}}\right)^{194^{8}}$$

$$= (((((((((((((((((2088^{878})^{878})^{878})^{878})^{878})^{878})^{276})^{276})^{276})^{194})^{194})^{194})^{194})^{194})^{194})^{194})^{194}$$

$$= 1317 (\mathrm{mod}\, 2773)$$

$$K_{ki} = \left(\left(13^{652^{3}}\right)^{1288^{5}}\right)^{778^{9}}$$

$$= (((((((((((((((((13^{652})^{652})^{652})^{1288})^{1288})^{1288})^{1288})^{1288})^{778})^{778})^{778})^{778})^{778})^{778})^{778})^{778})^{778}$$

$$= 1317 (\mathrm{mod}\, 2773)$$

FIG. 12

$$K_{jk} = K_{kj}$$

$$K_{jk} = \left(\left(1689^{256^{6}}\right)^{138^{3}}\right)^{76^{8}}$$

$$= (((((((((((((((((1689^{256})^{256})^{256})^{256})^{256})^{256})^{138})^{138})^{138})^{76})^{76})^{76})^{76})^{76})^{76})^{76})^{76}$$

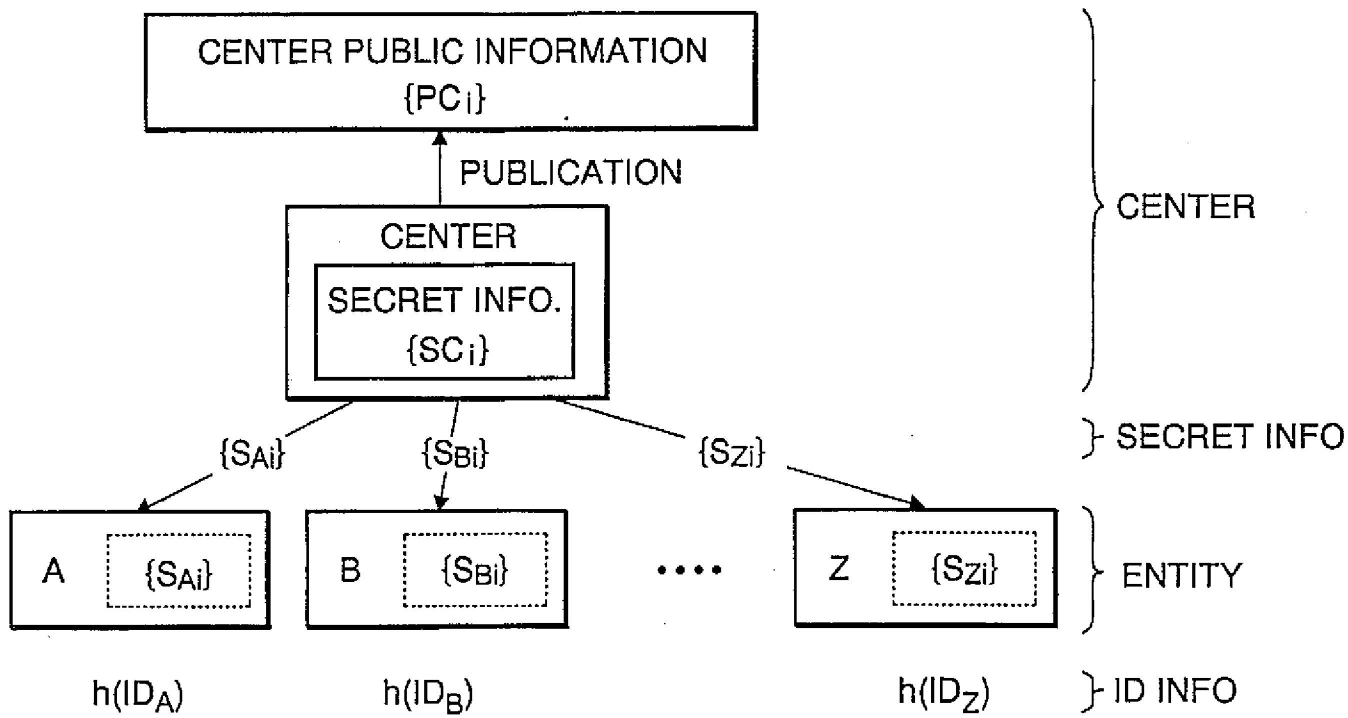
$$= 753 \pmod{2773}$$

$$K_{kj} = \left(\left(13^{652^{4}}\right)^{1288^{11}}\right)^{778^{2}}$$

$$= (((((((((((((((((13^{652})^{652})^{652})^{652})^{1288})^{1288})^{1288})^{1288})^{1288})^{1288})^{1288})^{1288})^{1288})^{1288})^{1288})^{778})^{778}$$

$$= 753 \pmod{2773}$$

FIG. 13



CENTER PUBLIC INFORMATION
{PCi}
PUBLICATION
CENTER
SECRET INFO.
{SCi}
CENTER
{SAi}
{SBi}
{SZi}
SECRET INFO
A
{SAi}
B
{SBi}
Z
{SZi}
ENTITY
h(IDA)
h(IDB)
h(IDZ)
ID INFO

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-317733
(43)Date of publication of application : 16.11.1999

(51)Int.Cl. H04L 9/08
G09C 1/00

(21)Application number : 10-125086
(22)Date of filing : 07.05.1998

(71)Applicant : MURATA MACH LTD
KASAHARA MASAO
FUJIKAWA ATSUNORI

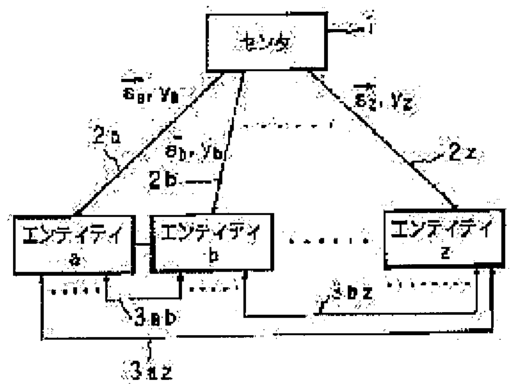
(72)Inventor : KASAHARA MASAO
FUJIKAWA ATSUNORI
MURAKAMI YASUMICHI

(54) CIPHER COMMUNICATION METHOD, CIPHERING METHOD, AND CIPHER COMMUNICATION SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a cipher communication method based on new ID-NIKS of very high safety which reveals to secret parameter of a center and disables a ciphertext to be deciphered even if entities conspire.

SOLUTION: In the method, there are 1st keys (open key) which are based upon the pieces of ID information of respective entities, made open, and unique to the entities, 2nd keys (secret key) which are found at the center 1 from the 1st keys of the entities with a 1st function and unique to the entities, and 3rd keys (common key) which are represented with a 2nd function of two variables, i.e., the 2nd key of one entity and the 2nd key of a partner, used to cipher a plaintext into a ciphertext and vise versa, and common to the two entities; and the 1st function including as parameters random numbers unique to the respective entities which are managed at the center 1 and a 3rd function which is obtained by substituting the 1st function in the 2nd function and includes as variables the 1st keys of one entity and a partner are functions that can not be separated as to the respective variables.



LEGAL STATUS

[Date of request for examination]	15.10.1999
[Date of sending the examiner's decision of rejection]	14.10.2003
[Kind of final disposal of application other than the examiner's decision of rejection or	

application converted registration]	
[Date of final disposal for application]	
[Patent number]	
[Date of registration]	
[Number of appeal against examiner's decision of rejection]	2003-022130
[Date of requesting appeal against examiner's decision of rejection]	13.11.2003
[Date of extinction of right]	

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報**（Ａ）　(11)特許出願公開番号 (Publication No.)

特開平11－317733

(43)公開日　平成11年(1999)11月16日 (publication date)

(51)Int.Cl.⁶		識別記号	ＦＩ		
Ｈ０４Ｌ	9/08		Ｈ０４Ｌ	9/00	６０１Ｄ
Ｇ０９Ｃ	1/00	６３０	Ｇ０９Ｃ	1/00	６３０Ｄ
					６３０Ｅ
			Ｈ０４Ｌ	9/00	６０１Ｅ

審査請求　未請求　請求項の数９　ＯＬ　（全 17 頁）

(21)出願番号　特願平10－125086

(22)出願日　平成10年(1998) ５月７日

特許法第30条第１項適用申請有り　平成10年１月28日～１月31日　電子情報通信学会情報セキュリティ研究専門委員会主催の「1998年暗号と情報セキュリティシンポジウム」において文書をもって発表

(71)出願人　000006297
村田機械株式会社
京都府京都市南区吉祥院南落合町３番地

(71)出願人　597008636
笠原　正雄
大阪府箕面市粟生外院４丁目15番３号

(71)出願人　597008647
藤川　篤則
東京都町田市中町２－２－８

(72)発明者　笠原　正雄
大阪府箕面市粟生外院４丁目15番３号

(74)代理人　弁理士　河野　登夫

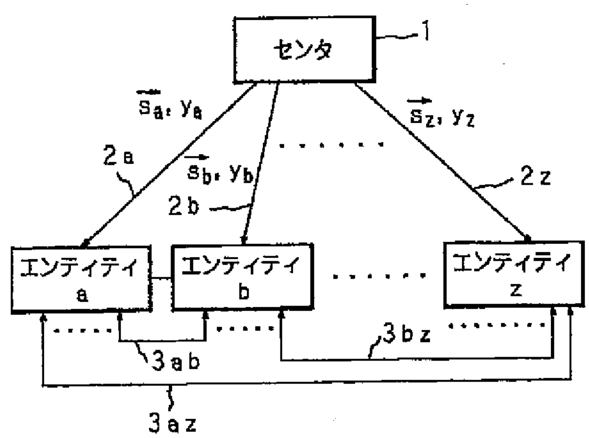
最終頁に続く

(54)【発明の名称】　暗号通信方法及び暗号化方法並びに暗号通信システム

(57)【要約】

【課題】　エンティティが結託してもセンタの秘密パラメータが露呈することなく暗号文が復号されず、安全性が極めて高い新規のＩＤ－ＮＩＫＳによる暗号通信方法を提供する。

【解決手段】　各エンティティのＩＤ情報に基づく公開された各エンティティ固有の第１の鍵（公開鍵）と、センタ１にてエンティティの第１の鍵から第１の関数にて求められる各エンティティ固有の秘密の第２の鍵（秘密鍵）と、自身の第２の鍵及び相手の第１の鍵の２変数による第２の関数で表され、平文を暗号文に暗号化する際及び暗号文を平文に復号する際に用いる２人のエンティティ間に共有する第３の鍵（共有鍵）とが存在し、センタ１が管理する各エンティティ固有の乱数をパラメータとした第１の関数と、第２の関数に第１の関数を代入して得られる、自身及び相手の第１の鍵を変数とする第３の関数とが、それぞれの変数について分離不可能な関数である。



【特許請求の範囲】

【請求項１】　センタから各エンティティへ各エンティティ固有の秘密鍵を送付し、一方のエンティティが前記センタから送付された該エンティティ固有の秘密鍵と公開された他方のエンティティの公開鍵とを利用して平文を暗号文に暗号化して他方のエンティティへ伝送し、該他方のエンティティが伝送された暗号文を前記センタから送付された該エンティティ固有の秘密鍵と公開された前記一方のエンティティの公開鍵とを利用して元の平文に復号することにより、エンティティ間で情報の通信を行う暗号通信方法において、前記公開鍵としての公開された各エンティティ固有の第１の鍵と、各エンティティの第１の鍵から第１の関数にて前記センタで求められる、前記秘密鍵に関連する各エンティティ固有の秘密の第２の鍵と、自身の第２の鍵及び相手の第１の鍵の２変数で示される第２の関数で表され、平文を暗号文に暗号化する際及び暗号文を平文に復号する際に用いる両エンティティ間で共有する第３の鍵とを使用して、エンティティ間で暗号化した情報の通信を行うこととし、前記センタが管理する各エンティティ固有の乱数をパラメータとした第１の関数と、第２の関数に第１の関数を代入して得られる、自身及び相手の第１の鍵を変数とする第３の関数とを、それぞれの変数について下記に定義される分離不可能な関数に設定することを特徴とする暗号通信方法。

定義：適当な可換な算法を○として、関数ｆ（・）がｆ（ｘ＋ｙ）≠ｆ（ｘ）○ｆ（ｙ）を満たす場合に、関数ｆ（・）は算法○により分離不可能である。

【請求項２】　前記第２の鍵は、各エンティティ固有の第１の鍵と前記センタが管理する対称行列とから生成される第１秘密鍵と、第１秘密鍵に乱数を乗じて生成される第２秘密鍵と、乱数に基づいて生成される第３秘密鍵とを含み、前記センタは生成した第２秘密鍵及び第３秘密鍵を各エンティティに送付し、一方のエンティティにて、第２秘密鍵及び第３秘密鍵と他方のエンティティの第１の鍵とを用いて第３の鍵を生成することを特徴とする請求項１記載の暗号通信方法。

【請求項３】　前記センタにおける第１秘密鍵，第２秘密鍵及び第３秘密鍵を生成する際の演算式は以下であることを特徴とする請求項２記載の暗号通信方法。

【数１】

$$\vec{x_i} \equiv \mathrm{T}^{\vec{v_i}} \pmod{L}$$

$$\vec{s_i} \equiv r_i \cdot \vec{x_i} \pmod{L}$$

$$y_i \equiv g^{r_i^{-e}} \pmod{N}$$

但し、

ベクトルｖｉ：エンティティｉの第１の鍵

ベクトルｘｉ：エンティティｉの第１秘密鍵

ベクトルｓｉ：エンティティｉの第２秘密鍵

ｙｉ：エンティティｉの第３秘密鍵

ｒｉ：エンティティｉの乱数

Ｌ：Ｌ＝λ（Ｎ）

Ｎ：Ｎ＝ＰＱ（Ｐ，Ｑは素数）

Ｔ：対称行列（各成分はＬと互いに素）

ｇ：Ｎを法とする最大生成元

ｅ：Ｌと互いに素な整数

λ（・）：Carmichael関数

【請求項４】　一方のエンティティにおいて第２秘密鍵及び第３秘密鍵と他方のエンティティの第１の鍵とに基づき第３の鍵を生成する際の演算式は以下であることを特徴とする請求項３記載の暗号通信方法。

【数２】

$$\begin{aligned}
K_{ij} &\equiv (\cdots((\overbrace{\cdots((\overbrace{\cdots(y_i^{s_{i1}})\cdots}^{v_{j1}})^{s_{i2}})\cdots}^{v_{j2}})^{s_{in}})\overbrace{\cdots)^{s_{in}}}^{v_{jn}} \\
&\equiv y_i^{\overbrace{s_{i1}\cdots s_{i1}}^{v_{j1}}\overbrace{s_{i2}\cdots s_{i2}}^{v_{j2}}\cdots\overbrace{s_{in}\cdots s_{in}}^{v_{jn}}} \\
&\equiv y_i^{{}^t\vec{s_i}\,\vec{v_j}} \\
&\equiv y_i^{\left(\prod_{k=1}^{n} r_i^{v_{ik}}\right)\cdot{}^t\vec{x_i}\,\vec{v_j}} \\
&\equiv y_i^{r_i^{\left(\sum_{k=1}^{n} v_{ik}\right)}\cdot{}^t\vec{x_i}\,\vec{v_j}} \\
&\equiv y_i^{r_i^{e}\cdot{}^t\vec{x_i}\,\vec{v_j}} \\
&\equiv g^{r_i^{-e}\cdot r_i^{e}\cdot{}^t\vec{x_i}\,\vec{v_j}} \\
&\equiv g^{{}^t\vec{x_i}\,\vec{v_j}} \\
&\equiv g^{{}^t\vec{v_i}\,\mathrm{T}\,\vec{v_j}} \pmod{N}
\end{aligned}$$

【請求項５】　各エンティティの特定情報をハッシュ関数を利用して計算することにより、各エンティティ固有の第１の鍵を求めることを特徴とする請求項１～４の何れかに記載の暗号通信方法。

【請求項６】　センタから各エンティティへ各エンティティ固有の秘密鍵を送付し、エンティティが前記センタから送付された該エンティティ固有の秘密鍵を利用して平文を暗号文に暗号化する暗号化方法において、公開された各エンティティ固有の第１の鍵と、前記センタにてエンティティの第１の鍵から第１の関数にて求められる各エンティティ固有の秘密の第２の鍵と、暗号化するエ

ンティティ自身の第２の鍵及び暗号文の送信先である相手エンティティの第１の鍵の２変数による第２の関数で表され、平文を暗号文に暗号化する際に用いる第３の鍵とを使用して、平文を暗号文に暗号化することとし、前記センタが管理する各エンティティ固有の乱数をパラメータとした第１の関数と、第２の関数に第１の関数を代入して得られる、自身及び相手の第１の鍵を変数とする第３の関数とを、それぞれの変数について下記に定義される分離不可能な関数に設定することを特徴とする暗号化方法。

定義：適当な可換な算法を○として、関数ｆ（・）がｆ（ｘ＋ｙ）≠ｆ（ｘ）○ｆ（ｙ）を満たす場合に、関数ｆ（・）は算法○により分離不可能である。

【請求項７】　情報である平文を暗号文に暗号化して送信する処理、及び、送信された暗号文を元の平文に復号する処理を相互に行う複数のエンティティと、各エンティティへ各エンティティ固有の秘密鍵を送付するセンタとを備えた暗号通信システムにおいて、公開された各エンティティ固有の第１の鍵から第１の関数により各エンティティ固有の秘密の第２の鍵を求めるセンタと、自身の第２の鍵及び通信相手の第１の鍵の２変数による第２の関数で表され、平文を暗号文に暗号化する際及び暗号文を平文に復号する際に用いる第３の鍵を求める複数のエンティティとを有し、前記センタが管理する各エンティティ固有の乱数をパラメータとした第１の関数と、第２の関数に第１の関数を代入して得られる、自身及び通信相手の第１の鍵を変数とする第３の関数とを、それぞれの変数について下記に定義される分離不可能な関数とすべくなしてあることを特徴とする暗号通信システム。

定義：適当な可換な算法を○として、関数ｆ（・）がｆ（ｘ＋ｙ）≠ｆ（ｘ）○ｆ（ｙ）を満たす場合に、関数ｆ（・）は算法○により分離不可能である。

【請求項８】　前記第２の鍵は、第１秘密鍵，第２秘密鍵及び第３秘密鍵を含み、前記センタは、各エンティティ固有の第１の鍵と前記センタが管理する対称行列とから第１秘密鍵を計算する手段と、第１秘密鍵に乱数を乗じて第２秘密鍵を計算する手段と、前記乱数に基づいて第３秘密鍵を計算する手段とを備え、計算された第２秘密鍵及び第３秘密鍵が各エンティティに送付されるべく構成したことを特徴とする請求項７記載の暗号通信システム。

【請求項９】　前記各エンティティは、前記センタから送付された第２秘密鍵及び第３秘密鍵と通信相手の第１の鍵とから第３の鍵を計算する手段を備えることを特徴とする請求項８記載の暗号通信システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、情報の内容が当事者以外にはわからないように情報を暗号化して通信する安全性が高い暗号通信方法及びシステムに関する。

【０００２】

【従来の技術】高度情報化社会と呼ばれる現代社会では、コンピュータネットワークを基盤として、ビジネス上の重要な文書・画像情報が電子的な情報という形で伝送通信されて処理される。このような電子情報は、容易に複写が可能である、複写物とオリジナルとの区別が困難であるという性質があり、情報保全の問題が重要視されている。特に、「コンピュータリソースの共有」，「マルチアクセス」，「広域化」の各要素を満たすコンピュータネットワークの実現が高度情報化社会の確立に不可欠であるが、これは当事者間の情報保全の問題とは矛盾する要素を含んでいる。このような矛盾を解消するための有効な手法として、人類の過去の歴史上主として軍事，外交面で用いられてきた暗号技術が注目されている。

【０００３】暗号とは、情報の意味が当事者以外には理解できないように情報を交換することである。暗号において、誰でも理解できる元の文（平文）を第三者には意味がわからない文（暗号文）に変換することが暗号化であり、また、暗号文を平文に戻すことが復号であり、この暗号化と復号との全過程をまとめて暗号系と呼ぶ。暗号化の過程及び復号の過程には、それぞれ暗号化鍵及び復号鍵と呼ばれる秘密の情報が用いられる。復号時には秘密の復号鍵が必要であるので、この復号鍵を知っている者のみが暗号文を復号でき、暗号化によって情報の秘密性が維持され得る。

【０００４】暗号化鍵と復号鍵とは、等しくても良いし、異なっていても良い。両者の鍵が等しい暗号系は、共通鍵暗号系と呼ばれ、米国商務省標準局が採用したＤＥＳ（Data Encryption Standards)はその典型例である。また、両者の鍵が異なる暗号系の一例として、公開鍵暗号系と呼ばれる暗号系が提案された。この公開鍵暗号系は、暗号系を利用する各ユーザ（エンティティ）が暗号化鍵と復号鍵とを一対ずつ作成し、暗号化鍵を公開鍵リストにて公開し、復号鍵のみを秘密に保持するという暗号系である。公開鍵暗号系では、この一対となる暗号化鍵と復号鍵とが異なり、一方向性関数を利用することによって暗号化鍵から復号鍵を割り出せないという特徴を持たせている。

【０００５】公開鍵暗号系は、暗号化鍵を公開するという画期的な暗号系であって、高度情報化社会の確立に必要な上述した３つの要素に適合するものであり、情報通信技術の分野等での利用を図るべく、その研究が活発に行われ、典型的な公開鍵暗号系としてＲＳＡ暗号系が提案された。このＲＳＡ暗号系は、一方向性関数として素因数分解の困難さを利用して実現されている。また、離散対数問題を解くことの困難さ（離散対数問題）を利用した公開鍵暗号系も種々の手法が提案されてきた。

【０００６】また、各エンティティの住所，氏名等の個人を特定するＩＤ（Identity）情報を利用する暗号系が

提案された。この暗号系では、ＩＤ情報に基づいて送受信者間で共通の暗号化鍵を生成する。また、このＩＤ情報に基づく暗号技法には、（１）暗号文通信に先立って送受信者間での予備通信を必要とする方式と、（２）暗号文通信に先立って送受信者間での予備通信を必要としない方式とがある。特に、（２）の手法は予備通信が不要であるので、エンティティの利便性が高く、将来の暗号系の中枢をなすものと考えられている。

【０００７】この（２）の手法による暗号系は、ＩＤ－ＮＩＫＳ（ID-based non-interactive key sharing scheme)と呼ばれており、通信相手のＩＤ情報を用いて予備通信を行うことなく暗号化鍵を共有する方式を採用している。ＩＤ－ＮＩＫＳは、送受信者間で公開鍵，秘密鍵を交換する必要がなく、また鍵のリスト及び第三者によるサービスも必要としない方式であり、任意のエンティティ間で安全に通信を行える。

【０００８】図１３は、このＩＤ－ＮＩＫＳのシステムの原理を示す図である。信頼できるセンタの存在を仮定し、このセンタを中心にして共有鍵生成システムを構成している。図１１において、エンティティＸの名前，住所，電話番号等のＩＤ情報は、ハッシュ関数ｈ（・）を用いてｈ（ID_x）で表す。センタは任意のエンティティＸに対して、センタ公開情報｛PC_i｝，センタ秘密情報｛SC_i｝及びエンティティＸのＩＤ情報ｈ（ID_x）に基づいて、以下のように秘密情報S_{xi}を計算し、秘密裏にエンティティＸへ配布する。

$S_{xi}=F_i$（｛SC_i｝，｛PC_i｝，ｈ（ID_x））

【０００９】エンティティＸは他の任意のエンティティＹとの間で、暗号化，復号のための共有鍵K_{xy}を、エンティティＸ自身の秘密情報｛S_{xi}｝，センタ公開情報｛PC_i｝及び相手先のエンティティＹのＩＤ情報ｈ（ID_Y）を用いて以下のように生成する。

$K_{xy}=f$（｛S_{xi}｝，｛PC_i｝，ｈ（ID_Y））

また、エンティティＹも同様にエンティティＸへの鍵を共有鍵K_{yx}を生成する。もし常に$K_{xy}=K_{yx}$の関係が成立すれば、この鍵K_{xy}，K_{yx}をエンティティＸ，Ｙ間で暗号化鍵，復号鍵として使用できる。

【００１０】上述した公開鍵暗号系では、例えばＲＳＡ暗号系の場合にその公開鍵の長さは現在の電話番号の十数倍となり、極めて煩雑である。これに対して、ＩＤ－ＮＩＫＳでは、各ＩＤ情報を名簿という形式で登録しておけば、この名簿を参照して任意のエンティティとの間で共有鍵を生成することができる。従って、図１１に示すようなＩＤ－ＮＩＫＳのシステムが安全に実現されれば、多数のエンティティが加入するコンピュータネットワーク上で便利な暗号系を構築できる。このような理由により、ＩＤ－ＮＩＫＳが将来の暗号系の中心になると期待されている。

【００１１】

【発明が解決しようとする課題】通信相手のＩＤ情報を用いて予備通信を行うことなく暗号化鍵及び復号鍵となる共有鍵を互いに共有するようなＩＤ－ＮＩＫＳにあっては、複数のエンティティの結託等の攻撃に対して十分に安全であることが望まれる。しかしながら、以上のようなＩＤ－ＮＩＫＳにおいては、攻撃法が検討されて、適当な人数のエンティティが結託すればセンタの秘密パラメータが露呈するという問題を含んでいる。暗号学的に安全なＩＤ－ＮＩＫＳを構築できるか否かは、高度情報化社会に重要な問題であり、より理想的な暗号方式の探究が進められている。

【００１２】このような状況にあって、本発明者は、安全かつ簡単なＩＤ情報に基づく予備通信が不要で結託攻撃に強いＩＤ－ＮＩＫＳの暗号方式を提案している（特願平９－８９７２号）。この方式は、後述する共有鍵公開関数を分離不可能な関数とした特徴を有し、この特徴と離散対数問題の難しさとにその安全性の根拠を置いている。

【００１３】しかしながら、このＩＤ－ＮＩＫＳの暗号方式では、特殊な素数（Ｐ＝２ｐｑ＋１（ｐ，ｑ：大きな素数）で示される素数Ｐ）を用いる必要がある。この素数は実用上、十分多く存在していることは証明されているが、暗号システム上の設計の自由度が低いことは否めない。また、鍵共有の手順が２段階の計算ステップを踏まなけらばならず、その途中の段階で成立する有効な攻撃法が存在しないとは言い切れず、攻撃を受けやすい。この暗号方式には、このような問題点があり、改善の余地がある。

【００１４】本発明は斯かる事情に鑑みてなされたものでありエンティティが結託してもセンタの秘密パラメータが露呈することなく暗号文が復号されず、安全性が極めて高い新規のＩＤ－ＮＩＫＳによる暗号通信方法及び暗号通信システムを提供することを目的とする。

【００１５】本発明の他の目的は、先願の特願平９－８９７２号の方式における問題点を解決してその方式を改良し、設計の自由度を高め、より安全性を高くできる暗号通信方法及び暗号通信システムを提供することにある。

【００１６】

【課題を解決するための手段】請求項１に係る暗号通信方法は、センタから各エンティティへ各エンティティ固有の秘密鍵を送付し、一方のエンティティが前記センタから送付された該エンティティ固有の秘密鍵と公開された他方のエンティティの公開鍵とを利用して平文を暗号文に暗号化して他方のエンティティへ伝送し、該他方のエンティティが伝送された暗号文を前記センタから送付された該エンティティ固有の秘密鍵と公開された前記一方のエンティティの公開鍵とを利用して元の平文に復号することにより、エンティティ間で情報の通信を行う暗号通信方法において、前記公開鍵としての公開された各エンティティ固有の第１の鍵と、各エンティティの第１

の鍵から第１の関数にて前記センタで求められる、前記秘密鍵に関連する各エンティティ固有の秘密の第２の鍵と、自身の第２の鍵及び相手の第１の鍵の２変数で示される第２の関数で表され、平文を暗号文に暗号化する際及び暗号文を平文に復号する際に用いる両エンティティ間で共有する第３の鍵とを使用して、エンティティ間で暗号化した情報の通信を行うこととし、前記センタが管理する各エンティティ固有の乱数をパラメータとした第１の関数と、第２の関数に第１の関数を代入して得られる、自身及び相手の第１の鍵を変数とする第３の関数とを、それぞれの変数について下記に定義される分離不可能な関数に設定することを特徴とする。

定義：適当な可換な算法を○として、関数ｆ（・）がｆ（ｘ＋ｙ）≠ｆ（ｘ）○ｆ（ｙ）を満たす場合に、関数ｆ（・）は算法○により分離不可能である。特徴とする。

【００１７】請求項２に係る暗号通信方法は、請求項１において、前記第２の鍵は、各エンティティ固有の第１の鍵と前記センタが管理する対称行列とから生成される第１秘密鍵と、第１秘密鍵に乱数を乗じて生成される第２秘密鍵と、乱数に基づいて生成される第３秘密鍵とを含み、前記センタは生成した第２秘密鍵及び第３秘密鍵を各エンティティに送付し、一方のエンティティにて、第２秘密鍵及び第３秘密鍵と他方のエンティティの第１の鍵とを用いて第３の鍵を生成することを特徴とする。

【００１８】請求項３に係る暗号通信方法は、請求項２において、前記センタにおける第１秘密鍵，第２秘密鍵及び第３秘密鍵を生成する際の演算式は以下であることを特徴とする。

【００１９】

【数３】

$$\vec{x_i} \equiv \mathbf{T}^{\vec{v_i}} \pmod{L}$$

$$\vec{s_i} \equiv r_i \cdot \vec{x_i} \pmod{L}$$

$$y_i \equiv g^{r_i^{-*}} \pmod{N}$$

【００２０】但し、

ベクトルｖｉ ：エンティティｉの第１の鍵

ベクトルｘｉ ：エンティティｉの第１秘密鍵

ベクトルｓｉ ：エンティティｉの第２秘密鍵

ｙｉ ：エンティティｉの第３秘密鍵

ｒｉ ：エンティティｉの乱数

Ｌ：Ｌ＝λ（Ｎ）

Ｎ：Ｎ＝ＰＱ（Ｐ，Ｑは素数）

Ｔ：対称行列（各成分はＬと互いに素）

ｇ：Ｎを法とする最大生成元

ｅ：Ｌと互いに素な整数

λ（・）：Carmichael関数

【００２１】請求項４に係る暗号通信方法は、請求項３において、一方のエンティティにおいて第２秘密鍵及び第３秘密鍵と他方のエンティティの第１の鍵とに基づき第３の鍵を生成する際の演算式は以下であることを特徴とする。

【００２２】

【数４】

$$
\begin{aligned}
K_{ij} &\equiv (\cdots((\cdots((\cdots(y_i^{s_{i1}})\cdots)^{s_{i2}})\cdots)^{s_{in}})\cdots)^{s_{in}} \\
&\equiv y_i^{\overbrace{s_{i1}\cdots s_{i1}}^{v_{j1}}\overbrace{s_{i2}\cdots s_{i2}}^{v_{j2}}\cdots\overbrace{s_{in}\cdots s_{in}}^{v_{jn}}} \\
&\equiv y_i^{{}^t\vec{s_i}\,\vec{v_j}} \\
&\equiv y_i^{\left(\prod_{k=1}^{n} r_i^{v_{ik}}\right)\cdot{}^t\vec{x_i}\,\vec{v_j}} \\
&\equiv y_i^{r_i^{\left(\sum_{k=1}^{n} v_{ik}\right)}\cdot{}^t\vec{x_i}\,\vec{v_j}} \\
&\equiv y_i^{r_i^{*}\cdot{}^t\vec{x_i}\,\vec{v_j}} \\
&\equiv g^{r_i^{-*}\cdot r_i^{*}\cdot{}^t\vec{x_i}\,\vec{v_j}} \\
&\equiv g^{{}^t\vec{x_i}\,\vec{v_j}} \\
&\equiv g^{{}^t\vec{v_i}\,\mathbf{T}\,\vec{v_j}} \pmod{N}
\end{aligned}
$$

【００２３】請求項５に係る暗号通信方法は、請求項１～４の何れかにおいて、各エンティティの特定情報をハッシュ関数を利用して計算することにより、各エンティティ固有の第１の鍵を求めることを特徴とする。

【００２４】請求項６に係る暗号化方法は、センタから各エンティティへ各エンティティ固有の秘密鍵を送付し、エンティティが前記センタから送付された該エンティティ固有の秘密鍵を利用して平文を暗号文に暗号化する暗号化方法において、公開された各エンティティ固有の第１の鍵と、前記センタにてエンティティの第１の鍵から第１の関数にて求められる各エンティティ固有の秘密の第２の鍵と、暗号化するエンティティ自身の第２の鍵及び暗号文の送信先である相手エンティティの第１の鍵の２変数による第２の関数で表され、平文を暗号文に暗号化する際に用いる第３の鍵とを使用して、平文を暗号文に暗号化することとし、前記センタが管理する各エンティティ固有の乱数をパラメータとした第１の関数と、第２の関数に第１の関数を代入して得られる、自身及び相手の第１の鍵を変数とする第３の関数とを、それ

ぞれの変数について下記に定義される分離不可能な関数に設定することを特徴とする。

【０025】請求項７に係る暗号通信システムは、情報である平文を暗号文に暗号化して送信する処理、及び、送信された暗号文を元の平文に復号する処理を相互に行う複数のエンティティと、各エンティティへ各エンティティ固有の秘密鍵を送付するセンタとを備えた暗号通信システムにおいて、公開された各エンティティ固有の第１の鍵から第１の関数により各エンティティ固有の秘密の第２の鍵を求めるセンタと、自身の第２の鍵及び通信相手の第１の鍵の２変数による第２の関数で表され、平文を暗号文に暗号化する際及び暗号文を平文に復号する際に用いる第３の鍵を求める複数のエンティティとを有し、前記センタが管理する各エンティティ固有の乱数をパラメータとした第１の関数と、第２の関数に第１の関数を代入して得られる、自身及び通信相手の第１の鍵を変数とする第３の関数とを、それぞれの変数について下記に定義される分離不可能な関数とすべくなしてあることを特徴とする。

【００２６】請求項８に係る暗号通信システムは、請求項７において、前記第２の鍵は、第１秘密鍵，第２秘密鍵及び第３秘密鍵を含み、前記センタは、各エンティティ固有の第１の鍵と前記センタが管理する対称行列とから第１秘密鍵を計算する手段と、第１秘密鍵に乱数を乗じて第２秘密鍵を計算する手段と、前記乱数に基づいて第３秘密鍵を計算する手段とを備え、計算された第２秘密鍵及び第３秘密鍵が各エンティティに送付されるべく構成したことを特徴とする。

【００２７】請求項９に係る暗号通信システムは、請求項８において、前記各エンティティは、前記センタから送付された第２秘密鍵及び第３秘密鍵と通信相手の第１の鍵とから第３の鍵を計算する手段を備えることを特徴とする。

【００２８】以下、本発明の暗号通信方法におけるＩＤ－ＮＩＫＳの概念について説明する。

【００２９】まず、線形の概念を一般化して、関数における分離可能を次のように定義する。適当な可換な算法を○として、関数ｆ（・）が次の関係式を満たす場合に、その関数ｆ（・）は算法○により分離可能であると定義する。

ｆ（ｘ＋ｙ）＝ｆ（ｘ）○ｆ（ｙ）

例えば、ｆ（ｘ）＝ａｘ，ｆ（ｘ）＝a^x は、以下に示すように分離可能である。

ｆ（ｘ＋ｙ）＝ａ（ｘ＋ｙ）＝ａｘ＋ａｙ＝ｆ（ｘ）＋ｆ（ｙ）

ｆ（ｘ＋ｙ）＝a^{x+y} ＝a^x ・a^y ＝ｆ（ｘ）・ｆ（ｙ）

【００３０】また、行列のべき乗演算の定義を、以下のようにする。但し、各行列Ａ，Ｂ，Ｃはそれぞれｍ×ｌ，ｌ×ｎ，ｍ×ｎの行列とする。

【００３１】

【数５】

行列の右べき乗演算 $\mathbf{C} = \mathbf{A}^{\mathbf{B}}$ を

$$c_{ij} = \prod_{k=1}^{\ell} a_{ik}{}^{b_{kj}} \quad (i = 1, 2, \ldots, m, \quad j = 1, 2, \ldots, n)$$

と定義する． □

行列の左べき乗演算 $\mathbf{C} = {}^{\mathbf{A}}\mathbf{B}$ を

$$c_{ij} = \prod_{k=1}^{\ell} b_{kj}{}^{a_{ik}} \quad (i = 1, 2, \ldots, m, \quad j = 1, 2, \ldots, n)$$

と定義する． □

【００３２】また、行列の各成分ごとに積をとる演算＊を、以下のように定義する。但し、各行列Ａ，Ｂ，Ｃはｍ×ｎの行列とする。行列の成分積Ｃ＝Ａ＊Ｂを、

$c_{ij} = a_{ij} b_{ij}$ （ｉ＝１，２，…，ｍ，　ｊ＝１，２，…，ｎ）

と定義する。

【００３３】以上のような定義により、以下の性質が成り立つ。但し、ｔは行列の転置を意味する。

【００３４】

【数６】

1. ${}^{t}\left(\mathbf{A}^{\mathbf{B}}\right) = {}^{{}^{t}\mathbf{B}}\,{}^{t}\mathbf{A}$

2. $\left(\mathbf{A}^{\mathbf{B}}\right)^{\mathbf{C}} = \mathbf{A}^{\mathbf{BC}}$

3. $\left({}^{\mathbf{A}}\mathbf{B}\right)^{\mathbf{C}} = {}^{\mathbf{A}}\left(\mathbf{B}^{\mathbf{C}}\right)$

4. $(\mathbf{A} * \mathbf{B})^{\mathbf{C}} = \mathbf{A}^{\mathbf{C}} * \mathbf{B}^{\mathbf{C}}$

5. $\mathbf{A}^{(\mathbf{B}+\mathbf{C})} = \mathbf{A}^{\mathbf{B}} * \mathbf{A}^{\mathbf{C}}$

【００３５】次に、ＩＤ－ＮＩＫＳを実現するための条件及び安全なＩＤ－ＮＩＫＳであるための条件について考察する。但しｉ，ｊ，ｙ及びｚはエンティティを表

し、v_i は多くの場合にＩＤのハッシュ値であるエンティティｉの公開鍵（特許請求の範囲の第１の鍵）、s_i はエンティティｉの秘密鍵（特許請求の範囲の第２の鍵）、K_{ij} はエンティティｉが求めたエンティティｊとの共有鍵（特許請求の範囲の第３の鍵）とする。

【００３６】ＩＤ－ＮＩＫＳを実現するためには、以下の条件１～３の３つの条件が必要である。

【００３７】〔条件１（秘密鍵生成条件）〕センタは、秘密鍵生成関数ｆ（・）（特許請求の範囲の第１の関数）を用いて、エンティティｉの公開鍵 v_i から対応する秘密鍵 s_i を求めることができる。

$s_i = f(v_i)$

【００３８】〔条件２（共有鍵生成条件）〕共有鍵生成関数ｇ（・）（特許請求の範囲の第２の関数）を用いて、エンティティｉの秘密鍵 s_i とエンティティｊの公開鍵 v_j とから共有鍵 K_{ij} を求めることができる。

$K_{ij} = g(s_i, v_j)$

【００３９】〔条件３（鍵共有条件）〕エンティティｉがエンティティｊに対して生成する共有鍵 K_{ij} と、エンティティｊがエンティティｉに対して生成する共有鍵 K_{ji} とは等しい。

$K_{ij} = K_{ji}$

従って、共有鍵生成関数ｇ（・）に秘密鍵生成関数ｆ（・）を代入して得られる、公開鍵 v_i, v_j を変数とする共有鍵公開関数Ｆ（・）（特許請求の範囲の第３の関数）は対称関数である。

$F(v_i, v_j) = F(v_j, v_i)$

但し、

$F(v_i, v_j) = g(f(v_i), v_j) = g(s_i, v_j)$

【００４０】また、複数のエンティティの結託攻撃に対して安全なＩＤ－ＮＩＫＳを構成するためには、以下の条件４～６を満たせば良い。

【００４１】〔条件４（結託に対する秘密鍵の安全性）〕秘密鍵生成関数ｆ（・）は、以下に示すように分離不可能な関数である。

$f(x+y) \neq f(x) \bigcirc f(y)$

秘密鍵生成関数ｆ（・）が分離可能な関数である場合には、２人のエンティティｉ，ｊの秘密鍵 s_i, s_j による結託攻撃により、他のエンティティｚの秘密鍵 s_z が求められ、破られてしまう。例えば、$v_z = v_i + v_j$ と表された場合に、秘密鍵 s_i, s_j を準備しておけば、以下のようにして、エンティティｚの秘密鍵 s_z を求めることが可能である。

$s_z = f(v_z)$
$= f(v_i + v_j)$
$= f(v_i) \bigcirc f(v_j)$
$= s_i \bigcirc s_j$

【００４２】〔条件５（結託に対する共有鍵の安全性）〕共有鍵公開関数Ｆ（・）は、以下に示すように分離不可能な関数である。

$F(a, x+y) \neq F(a, x) \bigcirc F(a, y)$

〔条件３〕より、共有鍵公開関数Ｆ（・）は対称関数であるので、次式も成立する。

$F(x+y, a) \neq F(x, a) \bigcirc F(y, a)$

共有鍵公開関数Ｆ（・）が、が分離可能な関数である場合には、エンティティの結託に伴う共有鍵による結託攻撃により破られてしまう。エンティティｉ，ｊが結託して、$v_z = v_i + v_j$ と表される場合には、K_{iy}（$= g(s_i, v_y) = F(v_i, v_y)$）及び K_{jy}（$= g(s_j, v_y) = F(v_j, v_y)$）を準備しておけば、以下のようにして、エンティティｙ，ｚ間の共有鍵 K_{yz} を求めることができる。

$K_{yz} = F(v_y, v_z)$
$= F(v_y, v_i + v_j)$
$= F(v_y, v_i) \bigcirc F(v_y, v_j)$
$= F(v_i, v_y) \bigcirc F(v_j, v_y)$
$= K_{iy} \bigcirc K_{jy}$

【００４３】この条件５は非常に厳しく、途中の計算にかかわらず、鍵共有段階の関数形が分離可能となっているだけでは安全でないことを意味する。例えば、積和型ＩＤ－ＮＩＫＳまたはべき積型ＩＤ－ＮＩＫＳはこの条件を満たしていない。

【００４４】〔条件６（センタ秘密の安全性）〕いかなる攻撃によってもセンタ秘密は求められない。

【００４５】本発明では、先願と同様に第３の関数（共有鍵公開関数）を分離不可能な関数に設定する（条件５）と共に、各エンティティ固有の秘密の乱数をパラメータとして関数内に組み込んで第１の関数（秘密鍵生成関数）を分離不可能な関数に設定する（条件４）。本発明では、このような分離不可能な関数の特徴と、ＲＳＡ暗号と同等の攻撃の難しさとに、安全性の根拠を置いている。また、特殊な形の素数を予め準備しておく必要がなくて設計の自由度が高く、両エンティティが共有する第３の鍵（共有鍵）を求める計算ステップが１段階で済み攻撃を受け難く安全性が高い。

【００４６】

【発明の実施の形態】図１は、本発明の暗号通信システムの構成を示す模式図である。情報の隠匿を信頼できるセンタ１が設定されており、このセンタ１としては、例えば社会の公的機関を該当できる。このセンタ１と、この暗号系システムを利用するユーザとしての複数の各エンティティａ，ｂ，…，ｚとは秘密通信路２ａ，２ｂ，…，２ｚにより接続されており、この秘密通信路２ａ，２ｂ，…，２ｚを介してセンタ１から秘密の鍵情報が各エンティティａ，ｂ，…，ｚへ伝送されるようになっている。また、２人のエンティティの間には通信路３ab，３az，３bz，…が設けられており、この通信路３ab，３az，３bz，…を介して通信情報を暗号化した暗号文が互いのエンティティ間で伝送されるようになっている。

【００４７】以下に、本発明のＩＤ－ＮＩＫＳの実施の形態を説明する。まず、（センタ１での準備処理），（エンティティの登録処理），（エンティティ間の共有鍵の生成処理）の順序で、本発明の暗号系を説明する。

【００４８】（センタ１での準備処理）センタ１は以下の公開鍵及び秘密鍵を準備し、公開鍵を公開する。

公開鍵	Ｎ	Ｎ＝ＰＱ
	ｅ	Ｌと互いに素な比較的小さな整数
秘密鍵	Ｐ，Ｑ	大きな素数
	Ｌ	Ｌ＝λ（Ｎ）
	ｇ	Ｎを法とする最大生成元
	Ｔ	ｎ×ｎの対称行列（各成分はＬと互いに素）
	r_i	個人秘密乱数

【００４９】但し、λ（・）はCarmichael関数とする。また、エンティティのＩＤ情報からｎ次元の公開鍵ベクトルｖ（特許請求の範囲の第１の鍵）を計算するためのハッシュ関数ｈ（・）も同時に公開する。ハッシュ関数はデータ列を別のデータ列に変換する関数であり、一般的には長いデータ列を短いデータ列に変換する関数である。但し、このハッシュ関数を用いて公開鍵ベクトルｖを計算した場合に、全成分の和がｅとなるようにする。即ち、以下の式が成り立つ。但し、v_{ik}はベクトルv_iの第ｋ成分を示す。具体的には、公開鍵ベクトルｖが２値ベクトルである場合にはSchalkwijkアルゴリズムを用いればよいし、一般的には、（ｎ－１）個の成分をハッシュ値で求め、最後の１個の成分を全体の和がｅとなるように求めればよい。

【００５０】

【数７】

$$e=\sum_{k=1}^{n} v_{i_k}$$

【００５１】（エンティティの登録処理）エンティティｉに登録を依頼されたセンタ１は、準備した鍵とエンティティｉの公開鍵ベクトルv_i（＝ｈ（ID_i））とを用いて以下の計算を行って、エンティティｉのベクトルx_i（特許請求の範囲の第１秘密鍵）とベクトルs_i（特許請求の範囲の第２秘密鍵）とy_i（特許請求の範囲の第３秘密鍵）とを順次求め、求めたベクトルs_i及びy_iをエンティティｉへ秘密裏に送って、登録を完了する。この際、直接エンティティｉに個人秘密であるベクトルx_iを送らない。

【００５２】

【数８】

1. $\vec{x_i}$ を求める．

$$\vec{x_i} \equiv \mathbf{T}^{\vec{v_i}} \pmod{L}$$

2. L と互いに素な乱数 r_i を選び，$\vec{s_i}$ を求める．

$$\vec{s_i} \equiv r_i \cdot \vec{x_i} \pmod{L}$$

3. $r_i^{-e} (\mathrm{mod}\, L)$ を求め，y_i を求める．

$$y_i \equiv g^{r_i^{-e}} \pmod{N}$$

【００５３】（エンティティ間の共有鍵の生成処理）エンティティｉは、エンティティｊとの鍵共有を行うために、以下のような高速指数演算法をｅ回繰り返すことにより共有鍵K_{ij}（特許請求の範囲の第３の鍵）を求める。

【００５４】

【数９】

$$
\begin{aligned}
K_{ij} &\equiv (\overbrace{\cdots((\cdots((\cdots(y_i^{s_{i1}})\cdots)}^{v_{j1}}\overbrace{{}^{s_{i2}})\cdots)}^{v_{j2}}\cdots\overbrace{{}^{s_{in}})\cdots)^{s_{in}}}^{v_{jn}} \\
&\equiv y_i^{\overbrace{s_{i1}\cdots s_{i1}}^{v_{j1}}\overbrace{s_{i2}\cdots s_{i2}}^{v_{j2}}\cdots\overbrace{s_{in}\cdots s_{in}}^{v_{jn}}} \\
&\equiv y_i^{{}^t\overrightarrow{s_i}\overrightarrow{v_j}} \\
&\equiv y_i^{\left(\prod_{k=1}^{n} r_i^{v_{ik}}\right)\cdot{}^t\overrightarrow{x_i}\overrightarrow{v_j}} \\
&\equiv y_i^{r_i^{\left(\sum_{k=1}^{n} v_{ik}\right)}\cdot{}^t\overrightarrow{x_i}\overrightarrow{v_j}} \\
&\equiv y_i^{r_i^{c}\cdot{}^t\overrightarrow{x_i}\overrightarrow{v_j}} \\
&\equiv g^{r_i^{-c}\cdot r_i^{c}\cdot{}^t\overrightarrow{x_i}\overrightarrow{v_j}} \\
&\equiv g^{{}^t\overrightarrow{x_i}\overrightarrow{v_j}} \\
&\equiv g^{{}^t\overrightarrow{v_i}\mathrm{T}\overrightarrow{v_j}} \pmod N
\end{aligned}
$$

【００５５】次に、上述した暗号システムにおけるエンティティ間の情報の通信について説明する。図２は、２人のエンティティａ，ｂ間における情報の通信状態を示す模式図である。図２の例は、エンティティａが平文（メッセージ）Ｍを暗号文Ｃに暗号化してそれをエンティティｂへ伝送し、エンティティｂがその暗号文Ｃを元の平文（メッセージ）Ｍに復号する場合を示している。

【００５６】エンティティａ側には、エンティティｂの個人識別情報ID_bを入力し、ハッシュ関数を利用してベクトルv_b（公開鍵）を得る公開鍵生成器１１と、センタ１から送られる秘密のベクトルs_a及びy_aと公開鍵生成器１１からの公開鍵であるベクトルv_bとに基づいてエンティティａが求めるエンティティｂとの共有鍵K_{ab}を生成する共有鍵生成器１２と、共有鍵K_{ab}を用いて平文（メッセージ）Ｍを暗号文Ｃに暗号化して通信路３０へ出力する暗号化器１３とが備えられている。

【００５７】また、エンティティｂ側には、エンティティａの個人識別情報ID_aを入力し、ハッシュ関数を利用してベクトルv_a（公開鍵）を得る公開鍵生成器２１と、センタ１から送られる秘密のベクトルs_b及びy_bと公開鍵生成器２１からの公開鍵であるベクトルv_aとに基づいてエンティティｂが求めるエンティティａとの共有鍵K_{ba}を生成する共有鍵生成器２２と、共有鍵K_{ba}を用いて通信路３０から入力した暗号文Ｃを平文（メッセージ）Ｍに復号して出力する復号器２３とが備えられている。

【００５８】図３は、図２の共有鍵生成器１２（２２）の内部構成を示す図である。共有鍵生成器１２（２２）は、センタ１から送られるベクトルｓを記憶する第１レジスタ４１と、ベクトルｓの各成分を記憶する第２レジスタ４２と、センタ１から送られるｙを記憶する第３レジスタ４３と、公開鍵生成器１１（２１）から送られるベクトルｖを記憶する第４レジスタ４４と、ベクトルｖの各成分を記憶する第５レジスタ４５と、自然数Ｎを記憶する第６レジスタ４６と、第２，第３，第５，第６レジスタ４２，４４，４５，４６の出力を用いて、数９に示す指数演算を行う高速指数演算器４７とを有する。

【００５９】次に、動作について説明する。エンティティａからエンティティｂへ情報を伝送しようとする場合、まず、エンティティｂの個人識別情報ID_bが公開鍵生成器１１に入力されてベクトルv_b（公開鍵）が得られ、得られたベクトルv_bが共有鍵生成器１２へ送られる。また、センタ１から数８に従って求められたベクトルs_a及びy_aが共有鍵生成器１２へ入力される。図３に示す構成を有する共有鍵生成器１２にて、数９に従って共有鍵K_{ab}が求められ、暗号化器１３へ送られる。暗号化器１３において、この共有鍵K_{ab}を用いて平文（メッセージ）Ｍが暗号文Ｃに暗号化され、暗号文Ｃが通信路３０を介して伝送される。

【００６０】通信路３０を伝送された暗号文Ｃはエンティティｂの復号器２３へ入力される。エンティティａの個人識別情報ID_aが公開鍵生成器２１に入力されてベクトルv_a（公開鍵）が得られ、得られたベクトルv_aが共有鍵生成器２２へ送られる。また、センタ１から数８に従って求められたベクトルx_b及びy_bが共有鍵生成器２２へ入力される。図３に示す構成を有する共有鍵

生成器２２にて、数９に従って共有鍵 K_{ba} が求められ、復号器２３へ送られる。復号器２３において、この共有鍵 K_{ba} を用いて暗号文Ｃが平文（メッセージ）Ｍに復号される。

【００６１】次に、このような本発明の暗号系が、前述したＩＤ－ＤＩＫＳの実現性（条件１～条件３）及びＩＤ－ＤＩＫＳの安全性（条件４～条件６）を満たすことを検証する。

【００６２】（条件１について）秘密鍵生成関数ｆ（・）は、個人秘密乱数 r_i をパラメータとして以下のように定義され、この秘密鍵生成関数ｆ（・）を用いて、センタ１はエンティティの公開鍵から対応する秘密鍵を求めることができる。

【００６３】

【数１０】

$$f_{r_i}(\overrightarrow{v_i}) \equiv r_i \mathbf{T}^{\overrightarrow{v_i}} \pmod{L}$$

【００６４】（条件２について）共有鍵生成関数ｇ（・）は、以下のように定義され、一方のエンティティの秘密鍵と他方のエンティティの公開鍵とから共有鍵を生成できる。

【００６５】

【数１１】

$$\mathcal{G}(\{y_i, \overrightarrow{s_i}\}, \overrightarrow{v_j}) \equiv y_i^{{}^t\overrightarrow{s_i}\,\overrightarrow{v_j}} \pmod{N}$$

【００６６】（条件３について）共有鍵公開関数Ｆ（・）は、以下の式で定義され、センタ秘密行列Ｔが対称行列であるので、以下の式で示すように、Ｆ（・）は対称関数であって、互いのエンティティが生成する共有鍵は等しくなる。

【００６７】

【数１２】

$$\mathcal{F}(\overrightarrow{v_i}, \overrightarrow{v_j}) \equiv g^{{}^t\overrightarrow{v_i}\mathbf{T}\overrightarrow{v_j}} \pmod{N}$$

$$\begin{aligned}\mathcal{F}(\overrightarrow{x}, \overrightarrow{y}) &= g^{{}^t\overrightarrow{x}\mathbf{T}\overrightarrow{y}} \\ &= g^{{}^t\overrightarrow{y}\,{}^t\mathbf{T}\overrightarrow{x}} \\ &= \mathcal{F}(\overrightarrow{y}, \overrightarrow{x})\end{aligned}$$

$$\begin{aligned}\mathcal{F}(\overrightarrow{a}, \overrightarrow{x}+\overrightarrow{y}) &= g^{{}^t\overrightarrow{a}\mathbf{T}\overrightarrow{x}+\overrightarrow{y}} \\ &= g^{{}^t\overrightarrow{a}\mathbf{T}\overrightarrow{x}\cdot{}^t\overrightarrow{a}\mathbf{T}\overrightarrow{y}} \\ &\neq \mathcal{F}(\overrightarrow{a}, \overrightarrow{x}) \circ \mathcal{F}(\overrightarrow{a}, \overrightarrow{y})\end{aligned}$$

【００６８】（条件４について）秘密鍵生成関数ｆ（・）は、以下に示すように、パラメータｒを固定すれば分離可能な関数となるが、本発明の暗号方式ではそのパラメータｒの値が各エンティティ毎に異なっているので、秘密鍵生成関数ｆ（・）は分離不可能な関数である。

【００６９】

【数１３】

$$\begin{aligned}f_r(\overrightarrow{x}+\overrightarrow{y}) &= r\mathbf{T}^{\overrightarrow{x}+\overrightarrow{y}} \\ &= r(\mathbf{T}^{\overrightarrow{x}} * \mathbf{T}^{\overrightarrow{y}}) \\ &= r\mathbf{T}^{\overrightarrow{x}} * r\mathbf{T}^{\overrightarrow{y}} \\ &= f_r(\overrightarrow{x}) * f_r(\overrightarrow{y})\end{aligned}$$

【００７０】例えば、ベクトル v_x ≡ベクトル v_i ＋ベクトル v_j の場合、ベクトル x_x ≡ベクトル x_i ＊ベクトル x_j となるが、ベクトル x_i 自体をエンティティに配布せず、それに個人乱数 r_i を乗じたベクトル s_i を配布しているので、ベクトル s_x ≡ベクトル s_i ＊ベクトル s_j とならず、個人秘密であるベクトル s_x ，ベクトル x_x の何れも求めることができない。

【００７１】（条件５について）共有鍵公開関数Ｆ（・）は、以下の式で示されるように、分離不可能な関数であるので、複数のエンティティの結託によって、公開鍵と秘密鍵とをいくら集めても、他のいかなるエンティティ間の共有鍵を求められない。

【００７２】

【数１４】

【0073】（条件6について）センタ秘密（P，Q，L，g，r_i 及びT）は、複数のエンティティが結託しても露呈しない。センタ秘密の中のP，Q，L，g，及びr_i が露呈しない根拠は以下の通りである。
P，Q，L：素因数分解の難しさ
g：r_i 未知による安全性
r_i ：合成数を法とする離散対数問題の難しさ
【0074】次に、センタ秘密行列Tの安全性について考察する。ここでは、結託したエンティティが各自の秘密鍵を持ち寄って高次連立合同式を解こうとする攻撃に対するセンタ秘密行列Tの安全性について考える。
【0075】本発明の暗号方式の場合、センタ秘密行列Tのn（n＋1）／2個のセンタ秘密変数に加え、更に個人乱数もセンタ秘密変数と考えて攻撃する必要がある。例えばm人のエンティティが結託したとすると、センタ秘密変数は｛n（n＋1）／2＋m｝個となる。この結果、任意の人数のエンティティが結託しても、センタ秘密行列Tを解くことは不可能である。以下、これが不可能である理由を、結託人数毎に分けて説明する。
【0076】（n人未満のエンティティが結託する場合）センタ秘密変数の数が、結託によって得られる線形独立な式の数を上回るので、センタ秘密行列Tを解くことができない。
【0077】（n人のエンティティが結託する場合）n人のエンティティが結託する場合には、最大で｛n（n＋1）／2＋（n－1）｝個の線形独立な式が得られる。一方、センタ秘密変数は｛n（n＋1）／2＋n｝個であるので、線形独立な式の数がセンタ秘密変数の数よりも1つ少なくなり、センタ秘密行列Tは解けない。
【0078】（（n＋1）人のエンティティが結託する場合）n人の場合に比べて新たに1つの個人秘密乱数が加わるが、その他のn項は線形従属であるので、新たな線形独立な式は1つしか得られない。このように、センタ秘密変数が1つ増加し、線形独立な式が1つ増加するだけであるので、n人の結託で解けなければ、（n＋1）人の結託でもセンタ秘密行列Tは解けない。
【0079】以上より、（n＋2）人以上のエンティティが結託しても、帰納的に、常に合同式の数は未知変数の数より1つ以上少ないので、解の不定性を除くことはできない。また、上記の連立合同式は一般に高次の連立合同式となり、解くことは難しい。更に、最終的にLを法とする逆元を乗ずる演算が必ず必要となり、法Lが分からない攻撃者にとって、これはRSA暗号を破ることに等しい。
【0080】また、もし仮に方程式を解くことなく合同式の数が未知変数の数よりも1つ少ないことを利用して一変数を消去できたとする。その場合、線型攻撃を利用することが考えられるが、攻撃したいエンティティのベクトルv_x は定重みベクトルであるので、他のエンティティの線型結合で表現するには必ず負の係数を必要とするため、この場合でも、法Lが分からない攻撃者にとって、RSA暗号を破ることに等しくなる。
【0081】以上のようにして、本発明の暗号方式では、センタ秘密行列Tが結託攻撃に対して安全であると言える。
【0082】ここで、個人乱数を設ける場合と個人乱数を設けない場合とにおけるセンタ秘密行列Tの安全性の具体例について説明する。図4は、個人乱数を設けず、5人のエンティティが結託した場合を示す。図4に示すように、5×5の行列Tは対称行列であるので、成分の未知数は15個である。また、図4に示すように、線形独立な式の数は5＋4＋3＋2＋1＝15となる。よって、未知数の個数と線形独立な式の数とが一致するため、解くことができ、センタ秘密行列Tが求められてしまうことになる。
【0083】一方、図5は、個人乱数を設け、5人のエンティティが結託した場合を示す。個人乱数もセンタ1側での秘密であるので、図5に示すように、未知数は行列T由来の15個と乱数由来の5個との合計20個である。また、図5に示すように、線形独立な式の数は5＋5＋4＋3＋2＝19となる。よって、未知数の個数が線形独立な式の数より多くなるため、解くことができず、センタ1の秘密が求められない。図6に、この場合の方程式を示す。
【0084】次に、本発明の暗号通信方法における数値例について説明する。図7，図8に第1の数値例（公開鍵ベクトルvの成分が2値であり、2人のエンティティi，jが鍵を共有する場合）を示す。まず、センタ1にて、図7（a）に示すように、公開鍵（N，e）及び秘密鍵（P，Q，L，g，T，r_i ，r_j ）を設定する。また、各エンティティi，jのIDに基づく2値の公開鍵ベクトルv_i ，v_jを計算して、図7（b）のように設定する。このような設定条件に基づいて、各エンティティi，jの$r_i{}^{-e}$，$r_j{}^{-e}$を求めると図7（c）のようになる。更に、エンティティiにおけるベクトルs_i ，y_i 及び共有鍵K_{ij}を求めると図8（a）に示すようになり、同様に、エンティティjにおけるベクトルs_j ，y_j 及び共有鍵K_{ji}を求めると図8（b）に示すようになる。
【0085】図9～図12に第2の数値例（公開鍵ベクトルvの成分が多値であり、3人のエンティティi，j，kが鍵を共有する場合）を示す。まず、センタ1にて、図9（a）に示すように、公開鍵（N，e）及び秘密鍵（P，Q，L，g，T，r_i ，r_j ，r_k ）を設定する。また、各エンティティi，j，kのIDに基づく多値の公開鍵ベクトルv_i ，v_j ，v_k を計算して、図9（b）のように設定する。このような設定条件に基づいて、各エンティティi，j，kの$r_i{}^{-e}$，$r_j{}^{-e}$，$r_k{}^{-e}$、ベクトルs_i ，s_j ，s_k 及びy_i ，y_j ，y_k を求めると図9（c）のようになる。そして、エンティティ

ティ ｉ，ｊ間の共有鍵$K_{ij}=K_{ji}$、エンティティｉ，ｋ間の共有鍵$K_{ik}=K_{ki}$、エンティティｊ，ｋ間の共有鍵$K_{jk}=K_{kj}$は、それぞれ、図１０，図１１，図１２のように求まる。

【００８６】

【発明の効果】以上詳述したように、本発明では、前述したＩＤ－ＮＩＫＳを実現するための３つの条件及びその安全性を確保するための３つの条件を満足するので、如何なる人数のエンティティが結託しても、センタの秘密パラメータは露呈されず暗号文が復号されることがなく、極めて高い安全性を達成できる。

【００８７】また、先願のように特殊な形の素数を予め準備しておく必要がなくなって設計の自由度が高くなり、また、鍵共有の手順が１段階の計算ステップで済み、先願よりも攻撃に対する安全性を高くできる。

【図面の簡単な説明】

【図１】本発明の暗号通信システムの構成を示す模式図である。

【図２】２人のエンティティ間における情報の通信状態を示す模式図である。

【図３】図２の共有鍵生成器の内部構成を示す図である。

【図４】個人乱数を設けない場合のセンタでの秘密の安全性を説明する図である。

【図５】個人乱数を設けた場合のセンタでの秘密の安全性を説明する図である。

【図６】本発明の安全性を表す数値例を示す図である。

【図７】本発明の第１の数値例を示す図である。

【図８】本発明の第１の数値例を示す図である。

【図９】本発明の第２の数値例を示す図である。

【図１０】本発明の第２の数値例を示す図である。

【図１１】本発明の第２の数値例を示す図である。

【図１２】本発明の第２の数値例を示す図である。

【図１３】ＩＤ－ＮＩＫＳのシステムの原理構成図である。

【符号の説明】

１ センタ

１１，２１ 公開鍵生成器

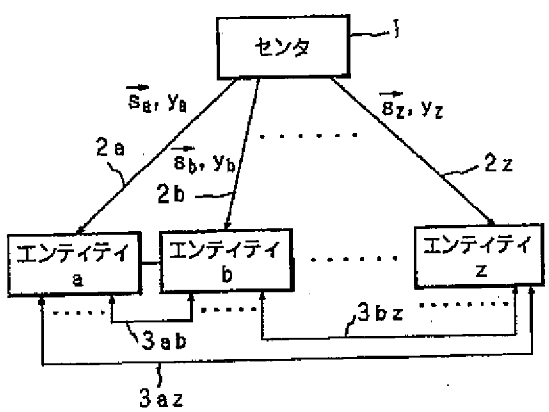
１２，２２ 共有鍵生成器

１３ 暗号化器

２３ 復号器

３０ 通信路

【図１】



【図４】

$$T=\begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ a_2 & b_1 & b_2 & b_3 & b_4 \\ a_3 & b_2 & c_1 & c_2 & c_3 \\ a_4 & b_3 & c_2 & d_1 & d_2 \\ a_5 & b_4 & c_3 & d_2 & e_1 \end{pmatrix}$$ ―未知数は１５個

$$\vec{v_1}=\begin{pmatrix}1\\0\\0\\0\\0\end{pmatrix},\ \vec{v_2}=\begin{pmatrix}0\\1\\0\\0\\0\end{pmatrix},\ \vec{v_3}=\begin{pmatrix}0\\0\\1\\0\\0\end{pmatrix},\ \vec{v_4}=\begin{pmatrix}0\\0\\0\\1\\0\end{pmatrix},\ \vec{v_5}=\begin{pmatrix}0\\0\\0\\0\\1\end{pmatrix}$$

$$\vec{x_i}=T\vec{v_i}$$

$$\vec{x_1}=\begin{pmatrix}a_1\\a_2\\a_3\\a_4\\a_5\end{pmatrix}\Big\}5 \quad \vec{x_3}=\begin{pmatrix}a_3\\b_2\\c_1\\c_2\\c_3\end{pmatrix}\Big\}3 \quad \vec{x_5}=\begin{pmatrix}a_5\\b_4\\c_3\\d_2\\e_1\end{pmatrix}\Big\}1$$

$$\vec{x_2}=\begin{pmatrix}a_2\\b_1\\b_2\\b_3\\b_4\end{pmatrix}\Big\}4 \quad \vec{x_4}=\begin{pmatrix}a_4\\b_3\\c_2\\d_1\\d_2\end{pmatrix}\Big\}2$$

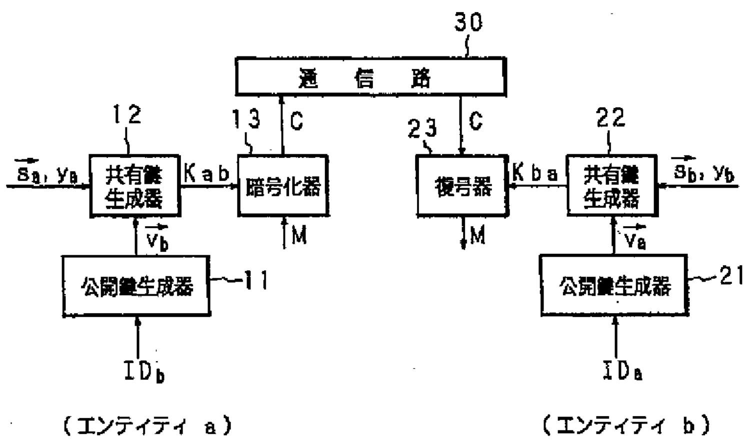
線形独立な式の数＝5+4+3+2+1=15

未知数15＝線形独立な式の数15

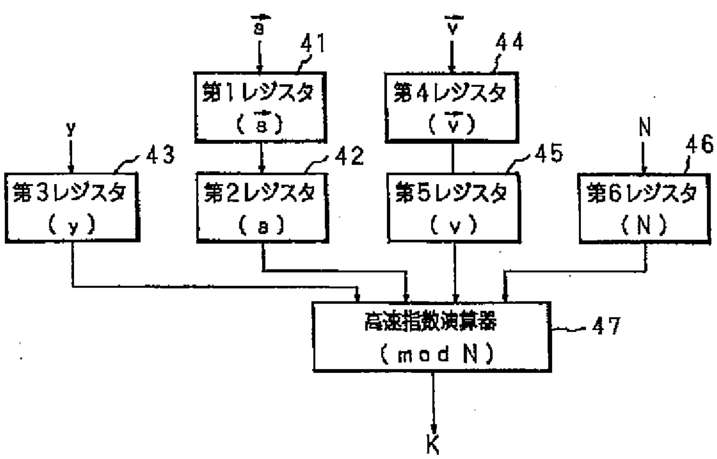
⇩

解ける

【図2】



【図3】



【図10】

$$K_{ij} = K_{ji}$$

$$
\begin{aligned}
K_{ij} &= \left(\left(2088^{878^4}\right)^{276^{11}}\right)^{194^2} \\
&= ((((((((((((((((2088^{878})^{878})^{878})^{878})^{276})^{276})^{276})^{276})^{276})^{276})^{276})^{276})^{276})^{276})^{276})^{194})^{194} \\
&= 189 \pmod{2773}
\end{aligned}
$$

$$
\begin{aligned}
K_{ji} &= \left(\left(1689^{256^3}\right)^{138^5}\right)^{76^9} \\
&= ((((((((((((((((1689^{256})^{256})^{256})^{138})^{138})^{138})^{138})^{138})^{76})^{76})^{76})^{76})^{76})^{76})^{76})^{76})^{76} \\
&= 189 \pmod{2773}
\end{aligned}
$$

【図５】

未知数は２０個

センタの秘密行列

$$T' = [T\,|\,R] = \left(\begin{array}{ccccc|ccccc} a_1 & a_2 & a_3 & a_4 & a_5 & r_1 & r_2 & r_3 & r_4 & r_5 \\ a_2 & b_1 & b_2 & b_3 & b_4 & r_1 & r_2 & r_3 & r_4 & r_5 \\ a_3 & b_2 & c_1 & c_2 & c_3 & r_1 & r_2 & r_3 & r_4 & r_5 \\ a_4 & b_3 & c_2 & d_1 & d_2 & r_1 & r_2 & r_3 & r_4 & r_5 \\ a_5 & b_4 & c_3 & d_2 & e_1 & r_1 & r_2 & r_3 & r_4 & r_5 \end{array}\right)$$

T' に対応する各エンティティの公開ベクトル

$$\vec{v_1} = \begin{pmatrix}1\\0\\0\\0\\0\\1\\0\\0\\0\\0\end{pmatrix}, \vec{v_2} = \begin{pmatrix}0\\1\\0\\0\\0\\0\\1\\0\\0\\0\end{pmatrix}, \vec{v_3} = \begin{pmatrix}0\\0\\1\\0\\0\\0\\0\\1\\0\\0\end{pmatrix}, \vec{v_4} = \begin{pmatrix}0\\0\\0\\1\\0\\0\\0\\0\\1\\0\end{pmatrix}, \vec{v_5} = \begin{pmatrix}0\\0\\0\\0\\1\\0\\0\\0\\0\\1\end{pmatrix}$$

$$\vec{s_i} = r_i T^{\vec{v_i}}$$

$$\vec{s_1} = \left.\begin{pmatrix}a_1 r_1\\a_2 r_1\\a_3 r_1\\a_4 r_1\\a_5 r_1\end{pmatrix}\right\} 5 \quad \vec{s_3} = \left.\begin{pmatrix}a_3 r_3\\b_2 r_3\\c_1 r_3\\c_2 r_3\\c_3 r_3\end{pmatrix}\right\} 4 \quad \vec{s_5} = \left.\begin{pmatrix}a_5 r_5\\b_4 r_5\\c_3 r_5\\d_2 r_5\\e_1 r_5\end{pmatrix}\right\} 2$$

$$\vec{s_2} = \left.\begin{pmatrix}a_2 r_2\\b_1 r_2\\b_2 r_2\\b_3 r_2\\b_4 r_2\end{pmatrix}\right\} 5 \quad \vec{s_4} = \left.\begin{pmatrix}a_4 r_4\\b_3 r_4\\c_2 r_4\\d_1 r_4\\d_2 r_4\end{pmatrix}\right\} 3$$

線形独立な式の数＝5+5+4+3+2=19

未知数２０＞線形独立な式の数19

⇩

解けない

【図７】

(a)

P=47, Q=59
N=2773, L=1334
g=2449, e=5
r_I=673, r_J=239

$$T = \begin{pmatrix} 547 & 416 & 360 & 309 & 339 & 288 & 396 & 470 \\ 416 & 359 & 303 & 252 & 280 & 210 & 341 & 409 \\ 360 & 303 & 241 & 194 & 224 & 173 & 288 & 351 \\ 309 & 252 & 194 & 139 & 173 & 120 & 234 & 178 \\ 339 & 280 & 224 & 173 & 197 & 148 & 262 & 331 \\ 288 & 210 & 173 & 120 & 148 & 101 & 210 & 275 \\ 396 & 341 & 288 & 234 & 262 & 210 & 331 & 393 \\ 470 & 409 & 351 & 178 & 331 & 275 & 393 & 457 \end{pmatrix}$$

(b)

$$\vec{v_I} = \begin{pmatrix}1\\0\\1\\0\\1\\1\\0\\1\end{pmatrix}, \vec{v_J} = \begin{pmatrix}0\\1\\1\\1\\0\\1\\1\\0\end{pmatrix}$$

(d)

r_I^{-e}=863
r_J=49

【図８】

(a)

エンティティＩ

$$\vec{s_I} = \begin{pmatrix}390\\340\\994\\292\\1054\\1314\\1086\\244\end{pmatrix} \quad \vec{v_J} = \begin{pmatrix}0\\1\\1\\1\\0\\1\\1\\0\end{pmatrix}, y_I = 1721$$

$$K_{IJ} = \left(\left(\left(\left(\left(1721^{340}\right)^{994}\right)^{292}\right)^{1314}\right)^{1086} = 51 \pmod{2773}$$

(b)

エンティティＪ

$$\vec{s_J} = \begin{pmatrix}954\\206\\1266\\914\\814\\454\\862\\72\end{pmatrix} \quad \vec{v_I} = \begin{pmatrix}1\\0\\1\\0\\1\\1\\0\\1\end{pmatrix}, y_J = 689$$

$$K_{JI} = \left(\left(\left(\left(\left(689^{954}\right)^{1266}\right)^{814}\right)^{454}\right)^{72} = 51 \pmod{2773}$$

【図６】

$$
\begin{pmatrix} x_1[1] \\ x_1[2] \\ x_1[3] \\ x_1[4] \\ x_1[5] \\ x_2[1] \\ x_2[2] \\ x_2[3] \\ x_2[4] \\ x_2[5] \\ x_3[1] \\ x_3[2] \\ x_3[3] \\ x_3[4] \\ x_3[5] \\ x_4[1] \\ x_4[2] \\ x_4[3] \\ x_4[4] \\ x_4[5] \\ x_5[1] \\ x_5[2] \\ x_5[3] \\ x_5[4] \\ x_5[5] \end{pmatrix}
=
\begin{pmatrix}
1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0\\
0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0\\
0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0\\
0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0\\
0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0\\
0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0\\
0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&1&0&0&0\\
0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&1&0&0&0\\
0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&1&0&0&0\\
0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&1&0&0&0\\
0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0\\
0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&1&0&0\\
0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&1&0&0\\
0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&1&0&0\\
0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&1&0&0\\
0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0\\
0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&1&0\\
0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&1&0\\
0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&1&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&1&0\\
0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1\\
0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&1\\
0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&1
\end{pmatrix}
\begin{pmatrix} a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ c_1 \\ c_2 \\ c_3 \\ d_1 \\ d_2 \\ e_1 \\ r'_1 \\ r'_2 \\ r'_3 \\ r'_4 \\ r'_5 \end{pmatrix}
$$

【図9】

(a)

$P=47, Q=59$

$N=2773, L=1334$

$g=2449, e=17$

$r_i=113, r_j=327, r_k=295$

$$T=\begin{pmatrix} 852 & 221 & 738 \\ 221 & 253 & 846 \\ 738 & 846 & 785 \end{pmatrix}$$

(b)

$$\vec{v_i}=\begin{pmatrix} 3 \\ 5 \\ 9 \end{pmatrix}, \vec{v_j}=\begin{pmatrix} 4 \\ 11 \\ 2 \end{pmatrix}, \vec{v_k}=\begin{pmatrix} 6 \\ 3 \\ 8 \end{pmatrix}$$

(c)

$r_i^{-e}=681, r_j^{-e}=641, r_k^{-e}=1115$

$$\vec{s_i}=\begin{pmatrix} 878 \\ 276 \\ 194 \end{pmatrix}, \vec{s_j}=\begin{pmatrix} 256 \\ 138 \\ 76 \end{pmatrix}, \vec{s_k}=\begin{pmatrix} 652 \\ 1288 \\ 778 \end{pmatrix}$$

$y_i=2088, y_j=1689, y_k=13$

【図11】

$$K_{ik}=K_{ki}$$

$$\begin{aligned} K_{ik} &= \left(\left(2088^{878^6}\right)^{276^3}\right)^{194^8} \\ &= (((((((((((((((2088^{878})^{878})^{878})^{878})^{878})^{276})^{276})^{276})^{194})^{194})^{194})^{194})^{194})^{194})^{194})^{194} \\ &= 1317 \pmod{2773} \end{aligned}$$

$$\begin{aligned} K_{ki} &= \left(\left(13^{652^3}\right)^{1288^5}\right)^{778^9} \\ &= ((((((((((((((((13^{652})^{652})^{652})^{1288})^{1288})^{1288})^{1288})^{1288})^{778})^{778})^{778})^{778})^{778})^{778})^{778})^{778})^{778} \\ &= 1317 \pmod{2773} \end{aligned}$$

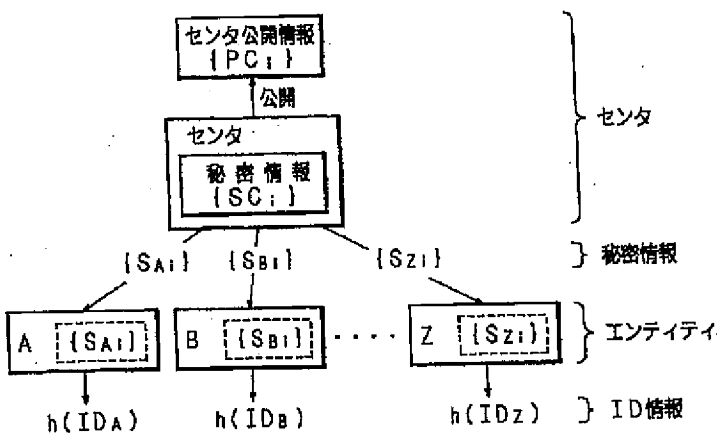
【図１２】

$$K_{jk} = K_{kj}$$

$$\begin{aligned}
K_{jk} &= \left(\left(1689^{256^{6}}\right)^{138^{3}}\right)^{76^{8}} \\
&= (((((((((((((((((1689^{256})^{256})^{256})^{256})^{256})^{256})^{138})^{138})^{138})^{76})^{76})^{76})^{76})^{76})^{76})^{76})^{76} \\
&= 753 \pmod{2773}
\end{aligned}$$

$$\begin{aligned}
K_{kj} &= \left(\left(13^{652^{4}}\right)^{1288^{11}}\right)^{778^{2}} \\
&= (((((((((((((((((13^{652})^{652})^{652})^{652})^{1288})^{1288})^{1288})^{1288})^{1288})^{1288})^{1288})^{1288})^{1288})^{1288})^{1288})^{778})^{778} \\
&= 753 \pmod{2773}
\end{aligned}$$

【図１３】



フロントページの続き

(72)発明者　藤川　篤則
東京都町田市中町２－２－８

(72)発明者　村上　恭通
京都府宇治市槇島町本屋敷51－６　村田機械株式会社社宅Ｂ棟602号